SSP 50021

Safety Requirements Document

International Space Station Program

December 12, 1995

National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas 77058

REVISION AND HISTORY PAGE

REV.	DESCRIPTION	PUB. DATE
-	Initial Release per SSCD 000353, EFF, 08-16-96	09-03-96

PREFACE

The International Space Station (ISS) Safety Requirements Document contains the safety requirements to be used by all United States and International Partner organizations involved in the design, development, production, test, and operation of ISS. The requirements contained herein represent the agreed standard by which the safety of ISS systems will be evaluated by the ISS Safety Review Panel, the Space Shuttle program management team, and the ISS program management team.

The contents of this document are intended to be consistent with the tasks and products to be prepared by the ISS participants as defined in SSP 30309 and as inplemented per SSP 30599. The ISS safety requirements shall be implemented on all ISS contractual and internal activities. This document is under the control of the Joint Program Requirements Control Board (JPRCB), and any changes or revisions will be approved by the JPRCB.

INTERNATIONAL SPACE STATION PROGRAM

SSP 50021
Concurrence

Prepared By:	Nicole Cloutier, Space Station Safety & Mission Assurance PRINT NAME	NS52 ORGN
	_____ SIGNATURE	12/12/95 DATE
Supervised By:	James Rush, Space Station Safety & Mission Assurance PRINT NAME	NS5 ORGN
	_____ SIGNATURE	12/12/95 DATE
Concurrence : (NASA))	Harold Taylor, Manager, Safety & Mission Assurance PRINT NAME	OE ORGN
	_____ SIGNATURE	12/12/95 DATE
Concurrence: (NASA)	Kevin A. Klein, Co-Chairman, ISSP SRP PRINT NAME	OE ORGN
	_____ SIGNATURE	12/12/95 DATE
Concurrence: (NASA)	A. M. Larsen, Co-Chairman, ISSP SRP PRINT NAME	MA ORGN
	_____ SIGNATURE	12/12/95 DATE
Approved By : (NASA)	Randy Brinkley, Manager, Space Station Program Office PRINT NAME	OA ORGN
	_____ SIGNATURE	12/12/95 DATE
Approved By : (NASA)	Tommy Holloway, Manager, Space Shuttle Program Office PRINT NAME	MA ORGN
	_____ SIGNATURE	12/xx/95 DATE

TABLE OF CONTENTS

1.0 INTRODUCTION

The ISS Program establishes the technical safety requirements for the design, development, test and operation of the International Space Station (ISS) End Items, Launch Packages (LPs), government furnished equipment (GFE), and their ground support equipment (GSE) through the ISS System Specification, SSP 41000, and the subsidiary segment and end item specifications. These specifications will continue to provide the safety requirements for ISS system developers, however, the ISS Prime contractor will be required to show traceability of the requirements herein to the appropriate ISS specifications for implementation and also assess compliance to the requirements herein using the results of the hazard analyses and ISS verification program. Joint documentation has been established to define the International Partner requirements. These documents are applicable to all ISS equipment provided by NASA, it's contractors, and the International Partners including support equipment. NSTS 1700.7B requirements applicable to ISS hardware and missions have been incorporated into this document. Appendix C provides tracibility between SSP 50021 and NSTS 1700.7 B.

The following documents were used as a basis to derive SSP 50021.

DOCUMENT NO.	TITLE
SSP 50005	International Space Station Flight Crew Integration Standard (NASA-STD-3000/T)
NSTS 1700.7B	Safety Policy and Requirements for Payloads Using the Space Transportation System
KHB 1700.7B	Space Shuttle Payload Ground Safety Handbook
SSP 30000 Section 3	Space Station Freedom Program Requirements Document, Safety, Reliability, Maintainability, and Quality Assurance Section
SSP 41000	ISS System Specification
SSP 41162	U.S. On-Orbit Segment Specification
SSP 41163	Russian Segment Specification
SSP 41165	Japanese Experiment Module Segment Specification
SSP 41167	Mobile Service System Segment Spcification
SSP 41160	Attached Pressurized Module Segment Specification
SSP 41164	Min-Pressurized Logistics Module Segment Specification
Various	U.S. Prime Item Development Specifications

1.1 PURPOSE

The purpose of SSP 50021 is to provide a single repository for the safety requirements found in the ISS System Specification, International Partner Segment Specifications and the United States Prime Item Development Specifications. The majority of the safety requirements are labeled as such in each specification section 3.3.6. There are, however, safety requirements scattered throughout the specifications. This repository of the safety requirements brings all the safety requirements into a single source and allows the Safety Review Panel to use it for assessing flight hardware compliance to the program safety requrements.

1.2 SCOPE

This document provides the requirements which are intended to protect flight and ground personnel, the ISS, the STS, payloads, GSE, the general public, public-private property, and the environment from ISS-related hazards. This document contains technical requirements applicable to ISS LP's during ground processing, launch, on-orbit flight operations, and return.

The requirements contained herein apply to ISS (USOS, NASA, RSA, ESA, NASDA, ASI, CSA) flight hardware and flight support equipment. Appendix C contains those implementations of the safety requirements for the International Partner implementation.

1.2.1 GSE DESIGN AND GROUND OPERATIONS

The requirements for ground support equipment design and operational safety are contained in Joint Space and Missile Test Organization (SAMTO)/Kennedy Space Center (KSC) Handbook, SAMTO HB S-100/KHB 1700.7, and SSP 50004 Ground Support Equipment Design Requirements.

1.2.2 MISSION RULES

Mission Rules will be prepared for each ISS mission that outline preplanned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. These mission rules are not additional safety requirements, but do define actions for completion of the ISS consistent with crew safety. Compliance with minimum safety requirements of this document will not insure the mission success of an ISS operation.

1.3 PRECEDENCE

In case of conflict between this document and an ISS Prime Item Development Specification or an International Partner Segment Specification, the applicable ISS specification shall take precedence.

1.4 DELEGATION OF AUTHORITY

Establishment and maintenance of this document is the responsibility of the Safety and Mission Assurance Office within the International Space Station Program Office (ISSPO). This document is subject to Joint Program Requirements Control Board (JPRCB) change control.

1.4.1 ISS

It is the responsibility of each ISS Program Participants (NASA, RSA, ESA, NASDA, ASI, CSA) to assure the safety of its end items and to implement the requirements of this document and identify any non-compliances with the applicable specification requirements or the requirements herein. The ISS Safety and Mission Assurance Office within the ISS Program Office is responsible for assuring the requirements herein are properly and completely included and allocated in the ISS specifications and requirements documents. The ISS Prime contractor will show traceability of the requirements herein to the corresponding requirement(s) in the ISS specifications and will evaluate compliance to this document. OE is responsible for maintenance and configuration control of this document.

1.5 WAIVERS AND DEVIATIONS

Requirements are imposed on flight hardware through the Segment Specifications for the International Partners and the Prime Item Development Specifications for the US hardware. Any request for waiver or deviation from the safety requirements in the Segment Specifications for the International Partners and the Prime Item Development Specifications for the US hardware will be considered as a waiver/deviation to the requirements herein. Request for waiver or deviation from this document shall be made to the ISS Program Office, in accordance with Configuration Management Requirements.

2.0 APPLICABLE AND REFERENCE DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The documents identified below are applicable to the extent specified herein. The references show where each applicable document is cited in this document.

No applicable documents have been identified.

2.2 REFERENCE DOCUMENTS

The documents identified below are referenced in this document and form a part of this document to the extent specified herein. The locations of each reference are identified.

DOCUMENT NO.	TITLE
ANSI-Z-136.1 Reference 3.3.6.7.1	American National Standard for Safe Use of Lasers
KHB 1700.7B Reference 1.2.1, 3.3.6.14	Space Transportation System Payload Ground Safety Handbook
MIL-STD-1522 Reference 3.2.10.11, 4.4.11	Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems
MIL-STD-1576 Reference 3.3.6.5.1.2	Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems All paragraphs except 5.12.3.1.e.
MSFC-DWG-20M02540 Reference Appendix C	Assessment of Flexible Line for Flow Induced Vibration
NSTS 07700, Vol. XIV Reference 3.3.6.12.3.1 3.3.6.13.6.4 3.3.6.13.7 3.3.6.13.8	System Description and Design Data - Extravehicular Activities Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb Attachment 1 (ICD 2-19001)
NSTS 08060 Reference 3.3.6.5.1.3	Space Shuttle System Pyrotechnic Specification
NSTS 08307 Reference 3.2.10.12	Criteria for Preloaded Bolts
NSTS 20793 Reference 3.3.6.8.4	Manned Space Vehicle, Battery Safety Handbook

NSTS-14046	Payload Verification Requirements
Reference 5.1.3.1	
SSP 30233	Space Station Requirements for Materials and Processes
Reference 3.2.9.1, 3.2.10.13	
SSP 30237	Space Station Electromagnetic Emission and Susceptibility Requirements for EMC
Reference 3.2.7.11	
SSP 30240	Space Station Grounding Standard Requirements
Reference 3.2.7.12	
SSP 30242	Space Station Cable/Wire Design and Control
Reference 3.2.7.18	Requirements for Electromagnetic Compatibility
SSP 30243	Space Station Systems Requirements for Electromagnetic Compatibility
Referrence 3.2.7.10,	
SSP 30245	Space Station Electrical Bonding Requirements
Reference 3.2.7.1.3	
SSP 30312	Electrical, Electronic, and Electromechanical (EEE) and Mechanical Parts Management and Implementation Plan for International Space Station Program
Reference 3.3.6.8.1.2	Appendix B, Section B3.5.2 (Wire and Cable Derating)
SSP 30425	Space Station Program Natural Environment Definition for Design
Reference 3.2.7.14	
SSP 30512	Space Station Ionizing Radiation Design Environment
Reference 3.2.7.15	

SSP 30558	Fracture Control Requirements for Space Station
Reference 3.3.6.4.1, 3.2.10.9 3.2.10.11, 3.2.10.15, 3.3	
SSP 30559	Structural Design and Verification Requirements
Reference 3.1.9.8, 4.4.1.1, 4.4.2.1	
SSP 30560	Glass, Window, and Ceramic Structural Design and Verification Requirements
Reference 3.2.10.10	
SSP 41141	Space Station Program Node Element 1 to U.S. Laboratory Element Interface Control Document
Reference 3.2.2.3.1.	
SSP 41143	Space Station Program Node Element 2 to U.S. Laboratory Element Interface Control Document
Reference 3.2.2.11	
SSP 42011	Integrated Truss Assembly (ITA) to Lab/Hab Interface Control Document
Reference 3.2.4.8	
SSP 50004	Ground Support Equipment Design Requirements
Reference 1.2.1, 3.3.6.14	
SSP 50005	International Space Station Flight Crew Integration Standard (NASA-STD-3000/T)
Reference	
3.3.6.6.1	Paragraphs 5.7.3.2 and 5.7.3.2.1
3.3.6.8.2	Paragraphs 6.3.3.1, Corner and edge requirements for
3.3.6.12.4.1	facilities and mounted equipment, 6.3.3.2, Exposed
3.3.6.12.5	corner requirements from facilities and mounted hardware and 6.3.3.11, Loose equipment.
	Section 6.4.3
	paragraph 14.3.
SSP 50011-01	Concept of Utilization (COU) REV. B Oct. 19, 1994
Reference 5.1	

SSP 50038 Computer Based Control System Safety Requirements

Reference 3.3.6.3.1

3.0 TECHNICAL REQUIREMENTS

The technical safety requriements in this document are grouped into three major sections; the safety requirements located in the ”Safety” section (paragraph 3.3.6) of the specifications, the safety requirements located in other sections of the specifications and the safety requirements located in the structural design documents. Although the numbers may be slightly different between specifications, the paragraph titles remains the same. Therefore, the section 3.1 will keep the paragraph numbers from 3.3.6, the second section, 3.2 will be grouped into like categories and the last section, 3.3, will maintain the exact paragraph numbers as they appear in SSP 30559 and SSP 30558. Paragraph numbers will be used for the second section, but will be assigned according to how they flow in this document. Any tables in SSP 50021 that are referenced from another document, have retained their original numbers from the source document.

3.1 SEGMENT SPECIFICATION AND PIDS SECTION 3.3.6 REQUIREMENTS

3.3.6 Safety

3.3.6.1 General

3.3.6.1.1 Catastrophic Hazards

The <END ITEM> shall be designed such that no combination of two failures, or two operator errors (See Appendix B), or one of each can result in a disabling or fatal personnel injury, or loss of the Orbiter or ISS. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls (See Appendix B) at the Segment/System levels.

3.3.6.1.2 Critical Hazards

The <END ITEM> shall be designed such that no single failure or single operator error can result in a nondisabling personnel injury, severe occupational illness; loss of a major ISS element on-orbit life sustaining function or emergency system, or involves damage to the Orbiter. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.3 Design for minimum risk

Hazards related to ”Design for Minimum Risk” (See Appendix B) areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or

factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of "Design for Minimum Risk" areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards

3.3.6.1.4.1 Inadvertent operation resulting in critical hazards

A function whose inadvertent operation could result in a critical hazard (See Appendix B) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of function resulting in critical hazards

Where loss of a function could result in a critical hazard, no single credible failure (See Appendix B) shall cause loss of that function and the function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function". Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards

3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards

Compliance with requirements a, b, and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See Appendix B), whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in catastrophic hazards

Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

b. The function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function"..

3.3.6.1.6 Subsequent induced loads

If a component of the <END ITEM> is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard.

3.3.6.1.7 Safety interlocks

Safety interlocks (See Appendix B) shall be provided to prevent unsafe operations when access to <END ITEM> equipment is required for maintenance.

3.3.6.1.8 Environmental compatibility

<End Item> functions shall be safe (See Appendix B) in the applicable worst case natural and induced environments defined in paragraph 3.2.5 "Environmental Conditions" or as defined in a payload integration plan , mission integration plan and/or interface control document.

3.3.6.2 Hazard Detection and Safing

3.3.6.2.1 Reserved

3.3.6.2.2 Monitors

3.3.6.2.2.1 Status information

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention

Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function.

3.3.6.2.2.3 Loss of input or failure

Loss of input or failure of the monitor shall be identifiable.

3.3.6.2.2.4 Launch site availability

Monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 Flight crew availability

Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

3.3.6.2.3 Near-real time monitoring

Near-real time monitoring (See Appendix B) of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, "Respond to Loss of Function". The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard.

3.3.6.2.4 Real Time Monitoring

3.3.6.2.4.1 Maintain status of hazard controls

The <End Item> shall provide real-time monitoring (See Appendix B) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the <End Item> is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground monitoring

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within the time to effect of the hazard upon loss of communication with the ground

3.3.6.3 Command and computer control of hazardous functions

3.3.6.3.1 Computer control of hazardous functions

The computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038.

3.3.6.4 Hazardous Materials

3.3.6.4.1 Hazardous fluid containment failure tolerance

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558.

3.3.6.4.2 Storage of Hazardous Chemicals.

Hazardous experiment payload chemicals/materials shall be stored only in International Standard Payload Racks (ISPRs) located in U.S. Laboratory or Logistics Modules.

3.3.6.5 Pyrotechnics

3.3.6.5.1 Pyrotechnics for USOS application

3.3.6.5.1.1 NASA Standard Initiators

NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions.

3.3.6.5.1.2 Firing circuit design

Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads.

3.3.6.5.1.3 Pyrotechnic operated devices

Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.

3.3.6.6 Radiation

Transmitters shall not irradiate the Orbiter at levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001). A two fault tolerant combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation of the Orbiter. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed Orbiter limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

3.3.6.7 Optics and Lasers

3.3.6.7.1 Lasers

Lasers used on <End Item>s shall be in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1.

3.3.6.7.2 Optical Requirements

3.3.6.7.2.1 Optical instruments

Optical instruments shall prevent harmful light intensities and wavelengths from being viewed by operating personnel.

3.3.6.7.2.2 Personnel protection

Quartz windows, apertures, or beam stops and enclosures shall be used for hazardous wavelengths and intensities unless suitable protective measures are taken to protect personnel form Ultraviolet or Infrared burns or X-Ray radiation.

3.3.6.7.2.3 Direct viewing optical systems

Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be limited to levels below the maximum permissible exposure (MPE).

3.3.6.8 Electrical Safety

3.3.6.8.1 Electrical power circuit overloads

3.3.6.8.1.1 Circuit overload protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination

a. <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

b. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock

The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3.

3.3.6.8.3 Reapplication of power

The <End Item> shall provide local control (See Appendix B) of interruption and reapplication of power to each IVA maintenance area.

3.3.6.8.4 Batteries

Batteries shall be designed to control application hazards caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of over temperature, shorts, reverse current, cell reversal, leakage, cell grounds, and over pressure. Safety guidelines for batteries are contained in NSTS 20793.

3.3.6.9 Cryogenics

3.3.6.9.1 Thermal characteristics

Cryogenic systems shall allow for component thermal expansion and contraction without imposing excessive loads on the system. Bellows, reactive thrust bellows, or other suitable load relieving flexible joints may be used.

3.3.6.9.2 Cryogenic entrapment

Anywhere a cryogenic can be trapped between any valves in the system, automatic relief shall be incorporated to preclude excess pressure from conversion from liquid to gaseous state causing a rupture.

3.3.6.9.3 Air compatibility

Cryogenic systems shall be insulated with an oxygen compatible material or be vacuum-jacketed to preclude liquefaction of air.

3.3.6.10 Fire Protection

a. The Space Station shall have the capability for crew initiated notification of a fire event within 1 minute after crew detection.

b. The Space Station shall assure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.

c. The Space Station shall accommodate the application of a fire suppressant at each enclosed location containing a potential fire source.

d. Fire suppressant shall be compatible with Space Station life support hardware, not reach toxic concentrations, and be noncorrosive.

e. Fire suppressant by-products shall be compatible with the Space Station life support contamination control capability.

f. Fixed fire suppression, where installed, shall incorporate a disabling feature to prevent inadvertent activation during maintenance.

g. One Portable Breathing Apparatus (PBA) and one Portable Fire Extinguisher (PFE) shall be located in elements less than or equal to 24 feet in accessible interior length. Where the element exceeds 24 feet in accessible interior length, a set of PBAs and PFEs shall be located within 12 feet of each end of the element. At least one PBA shall be located within three feet of each PFE.

h. Fixed fire suppression, where installed, shall be restorable after discharge.

i. Fixed fire suppression, where installed, shall remain functional after the removal of power to a location after detection of a fire event.

j. The Space Station shall confirm a fire event condition prior to any automated isolation, or suppression. Confirmation consists of at least two validated indications of fire/smoke from a detector.

k. On-board verification of suppressant availability shall be provided.

3.3.6.11 Constraints

3.3.6.11.1 Reserved

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance

3.3.6.11.2.1 Pressure differential tolerance

<END ITEM> equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard .

3.3.6.11.2.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards.

3.3.6.11.3. Emergency egress

The <End Item> shall provide for safe emergency IVA egress to the remaining contiguous pressurized volumes and have the capability to isolate from other flight pressurized volumes within three minutes, including closing hatches.

3.3.6.11.4. Reserved

3.3.6.11.5 Reserved

3.3.6.11.6 Component hazardous energy provision

Components which retain hazardous energy potential shall either be designed to prevent a crewmember conducting maintenance from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful.

3.3.6.11.7 Hatch opening

The <End Item> shall provide the capability to control pressure differential and verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels of selected compounds from Table 1 (See paragraph 3.2.2.7, Table VII) provide visual inspection of the interior of the pressurized volume prior to crew ingress.

3.3.6.11.8 Reserved

3.3.6.11.9 Reserved

3.3.6.11.10 Reserved

3.3.6.11.11 Reserved

3.3.6.11.12 Hazardous Gas Accumulation

3.3.6.11.12.1 Accumulation prevention

The <End Item> shall provide the capability to prevent uncontrolled hazardous accumulations of gases.

3.3.6.11.12.2 Detection, monitoring, and control

Detection, monitoring, and control of hazardous gases or vapors shall be required.

3.3.6.11.13 Equipment clearance for entrapment hazard

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Light Fixture

Light fixtures assemblies shall incorporate features to contain all glass fragments in the case of lamp breakage.

3.3.6.12 Human engineering safety

3.3.6.12.1 Internal volume touch temperature

3.3.6.12.1.1 Continuous contact - high temperature

Surfaces which are subject to continuous contact with crewmember bare skin and whose temperature exceeds 113 degrees Fahrenheit, shall be provided with guards or insulation to prevent crewmember contact.

3.3.6.12.1.2 Incidental or momentary contact - high temperature

For incidental or momentary contact (30 seconds or less), the following apply:

Crewmember warning - Surfaces which are subject to incidental or momentary contact with crewmember bare skin and whose temperatures are between 113 and 122 degrees Fahrenheit shall have warning labels that will alert crewmembers to the temperature levels.

Crewmember protection - Surface temperatures which exceed 122 degrees Fahrenheit shall be provided with guards or insulation that prevent crewmember contact.

3.3.6.12.1.3 Internal volume low touch temperature

When surfaces below 39 degrees Fahrenheit which are subject to continuous or incidental contact, are exposed to crewmember bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site.

3.3.6.12.2 External touch temperature

The suit shall be protected from high or low touch temperature extremes as follows:

3.3.6.12.2.1 Incidental contact

For incidental contact, temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates as specified in TableVII, " Heat Transfer Rates".

TABLE VII. Heat transfer rates

Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate(1) (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52(2)

	Incidental (0.5 max)	113	1.444	176.2(3)
Cold Object	Unlimited	40	1.062	-132.7(2)
	Incidental (0.5 max)	40	1.478	-325.2(3)

Notes:
1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

3.3.6.12.2.2 Unlimited contact

For unlimited contact, temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table VIII, limit heat transfer rates as specified in Table VII.

TABLE VIII. Designated EVA interfaces
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection

3.3.6.12.3.1 Sharp edges

<END ITEM> equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb.

3.3.6.12.3.2 Thin materials

Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches.

3.3.6.12.3.3 Planned maintenance or storage

Equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.1

3.3.6.12.4 Internal corner and edge protection

3.3.6.12.4.1 Equipment exposed to crew activity

Surfaces of <END ITEM> equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 Equipment exposed only during planned maintenance activities

Corners and edges of material, equipment or ORUs which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

3.3.6.12.5 Contingency repressurization

Controls necessary for restoring a depressurized module to normal operating pressurized conditions shall be capable of being manually operated by an EVA suited crewperson as specified in SSP 50005, paragraph 14.3.

3.3.6.12.6 Latches

Latches or similar devices shall be designed to prevent entrapment of crewmember appendages.

3.3.6.12.7 Screws and bolts

Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 Safety Critical Fasteners

Safety critical fasteners shall be designed to prevent inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

3.3.6.12.10 Burrs

Exposed surfaces shall be smooth and free of burrs.

3.3.6.12.11 Holes

3.3.6.12.11.1 Equipment located inside habitable volumes

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes.

3.3.6.12.11.2 Equipment located outside habitable volumes

Holes (round, slotted, polygonal) in EVA translation hand rails/holds shall be 1.0 inches or greater in diameter.

3.3.6.12.12 Protrusions

Equipment except for translation aids identified in Table VIII shall not protrude into the 50 inch horizontal by 72 inch vertical envelope of the CETA/MT corridor, or the 43 inch horizontal envelope of the primary and secondary translation path.

3.3.6.12.13 Pinch points

Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crewmember appendages.

3.3.6.12.14 Emergency Ingress

The <End Item> shall design EVA translation paths and aids such that an EVA crewmember can complete an emergency ingress within 30 minutes into a pressurized volume from EVA worksites on <End Item> hardware.

3.3.6.12.15 Reserved

3.3.6.12.16 Flexhoses

Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware.

3.3.6.12.17 Translation routes and established worksites

For protection from hazards along translation routes and established worksites the following apply:

3.3.6.12.17.1 Primary translation routes and established worksites

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.

b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.17.2 Secondary translation routes and established worksites

External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded and controlled as specified in Table X, “Control for exposed risks to EVA crew”.

TABLE X. Control for exposed risks to EVA crew		
Risk Type	Hazard	Control Method *
Innate Characteristics	Non-Ionizing Radiation (Antennas transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards
	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Connectors	Warning Strips and Placards
	Thermal (>235 degrees F or < -180 degrees F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards
	Narrow Passageways Protrusions	Placards
	Structure Sensitive to EVA Loads	Placards
	Pinch Points	Placards
	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards
CETA Corridor	Structural Impacts - Mobile Transporter - End of Rail	Color-coded Anodized yellow with black cross-hatching
Note: * Control methods shall be designed in accordance with SSP 50006.		

3.3.6.12.17.3 EVA crewmember contact isolation

<END ITEM> hardware which cannot be controlled by design features to comply with ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crewmember contact.

3.3.6.12.18 Moving or rotating equipment

The EVA crewmember shall be protected from moving or rotating equipment.

3.3.6.13 Launch vehicle interfaces and services

3.3.6.13.1 Safe Without Space Shuttle Program Services

3.3.6.13.1.1 Fault tolerance/safety margins

The <END ITEM> shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions

During Orbiter emergency conditions, <END ITEM> shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter Services

When Orbiter services are to be utilized to control <END ITEM> hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions

Inadvertent deployment, separation or jettison of the <END ITEM> or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4, 3.3.6.1.5 and 3.3.6.2.2 apply.

3.3.6.13.4 Planned Deployment/Extension Functions

3.3.6.13.4.1 Violation of Orbiter payload door envelope

If a component of the <END ITEM> or any <END ITEM> orbital support equipment (OSE) violates the payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance

The combination of these primary and backup methods shall be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency Return and Rapid Safing

The <End Item> shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop. For emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes. For a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements apply to <End Item> hardware with direct interfaces with the Orbiter:

3.3.6.13.5.1 Emergency de-orbit

The <End Item> hardware shall have at least one system to allow the Orbiter to meet the emergency de-orbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-<End Item> hardware operations.

3.3.6.13.5.2 Next primary landing site contingency deorbit

The <End Item> hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency deorbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-<End Item> hardware operations.

3.3.6.13.6 Flammable Atmosphere

3.3.6.13.6.1 Normal functions

During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) <END ITEM> functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical ignition sources

Electrical ignition sources shall not be exposed.

3.3.6.13.6.3 Surface temperatures

Surface temperatures shall be below 352 degrees F. (177.7 degrees C)

3.3.6.13.6.4 Conductive surfaces

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1.

3.3.6.13.7 Allowable RF radiation levels

<END ITEM> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.

3.3.6.13.8 Lightning protection

<END ITEM> electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard.

3.3.6.13.9 Orbiter vent/dump provisions

3.3.6.13.9.1 Release or ejection of hazardous material

<End Item> hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS.

3.3.6.13.9.2 Fluid system containment

<End Item> shall be designed to contain both hazardous and nonhazardous fluids when in the presence of the Orbiter.

3.3.6.13.10 Sealed Compartments

<End Item> components, located in regions of the Orbiter other than the habitable volume, shall be designed to withstand the decompression and repressurization enviroments associated with ascent or descent without resulting in a hazard.

3.3.6.14 Ground interfaces and services - Space Shuttle launch

Hazards shall not be created due to the inaccessibility of flight hardware such as:.

(a) Moving parts

Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.

(b) Equipment requiring adjustment

Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable.

(c) Ignition of adjacent materials

Electrical equipment shall not cause ignition of adjacent materials.

(d) Accidental contact with electrical equipment

Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.

3.2 ALL OTHER SECTIONS SAFETY REQUIREMENTS

This section contains end item requirements that are examples of the types of requirements that are needed for a complete set of safety requirements

3.2.1 Redundancy

3.2.1.1 Failure propagation

A single failure of an Orbital Replaceable Unit (ORU) in a functional path within the <End Item> shall not induce any other failures external to the failed ORU. [Lab PIDS 3.2.3.2]

3.2.1.2 Separation of redundant paths

Alternate or redundant functional paths shall be separated or protected such that any single credible event which causes the loss of one functional path will not result in the loss of the redundant functional path(s). Restrict assessment of compliance to safety critical redundancies.[Lab PIDS 3.2.3.3]

3.2.1.3 Failure tolerance

The International Space Station shall be one failure tolerant to prevent loss of an EVA crewmember due to inadvertent separation from International Space Station.

3.2.2 Characteristics

3.2.2.1 Performance Characteristics

Reserved

3.2.2.2 Monitor total pressure

The purpose of this function is to measure the total pressure of the USL atmosphere for control purposes. The USL shall monitor total pressure in the range of 0 to 16.0 psia with an accuracy of +/- 0.01 psia and report the cabin atmospheric pressure once per minute. The USL shall alert the

crew within one minute when the cabin atmosphere pressure drops below 13.9 psia for longer than three minutes. [Lab PIDS 3.2.1.1]

3.2.2.3 Introduce nitrogen

The purpose of this function is to provide a controlled release of gaseous nitrogen into the USL cabin atmosphere for maintenance and restoration of USL cabin pressure, and to maintain the cabin pressure in the USL and the attached pressurized modules in response to loss of cabin atmosphere to space. The USL must be supplied with gaseous nitrogen in order to perform this function. [Lab PIDS 3.2.1.2]

3.2.2.3.1

The USL shall provide remote and manual on/off control of introduction of gaseous nitrogen into the internal atmosphere of the USL at a flow rate of 0.1 to 0.2 lbm per min when supplied with gaseous nitrogen as specified in SSP 41141.

3.2.2.3.2

The USL shall provide the capability to maintain cabin total pressure at greater than 14.1 psia.This maintenance of cabin pressure by the USL shall not cause nitrogen partial pressure to exceed 11.6 psia, or cabin total pressure to exceed 14.9 psia.

3.2.2.3.3

The capability of the USL to maintain cabin pressure shall be subject to remote activation and deactivation by crew and ground.

3.2.2.3.4

The <End Item> shall be capable of maintaining the cabin pressure for the entire ISS in an open-hatch, active-IMV configuration when supplied with gaseous nitrogen as specified in SSP 41141.

3.2.2.3.5

The <End Item> shall be capable of maintaining the cabin pressure in a closed-hatch, closed-IMV US Lab when supplied with gaseous nitrogen as specified in SSP 41141.

3.2.2.4 Introduce oxygen

The purpose of this function is to provide a controlled release of gaseous oxygen into the <End Item> cabin atmosphere for maintenance and restoration of <End Item> cabin pressure, and to maintain the oxygen partial pressure in the <End Item> and the attached pressurized modules in response to metabolic consumption and loss of cabin atmosphere to space. The <End Item> must be supplied with gaseous oxygen in order to perform this function.

3.2.2.4.1

The <End Item> shall provide remote and manual on/off control of introduction of gaseous oxygen into the internal atmosphere of the <End Item> at a flow rate of 0.1 to 0.2 lbm per min when supplied with gaseous oxygen as specified in SSP 41141.

The <End Item> shall provide the capability to maintain oxygen partial pressure above 2.83 psia. This maintenance of oxygen partial pressure by the <End Item> shall not cause the oxygen partial pressure to exceed 3.35 psia or 24.1 percent by volume.

3.2.2.4.2

The capability of the <End Item> to maintain oxygen partial pressure shall be subject to remote activation and deactivation by crew and ground.

3.2.2.4.3

The <End Item> shall be capable of maintaining the oxygen partial pressure for the entire ISS in an open-hatch, active-IMV configuration and capable of maintaining the <End Item> oxygen pressure in a closed-hatch, closed-IMV US Lab when supplied with gaseous oxygen as specified in SSP 41141.

3.2.2.5 Relieve overpressure

The purpose of this function is to control the maximum internal-to-external differential pressure of the <End Item>.

3.2.2.5.1

The <End Item> shall control the maximum internal-to-external differential pressure of the USL to less than 15.2 psid. Venting of atmosphere to space shall not occur at less than 15.0 psia.

3.2.2.6 Equalize pressure

The purpose of this function is to allow equalization of pressure differential between the <End Item> and an adjacent, isolated volume.

3.2.2.6.1

The <End Item> shall equalize the pressure differential across internal hatches from a high of 14.9 psia on the USL side to a low of 14.1 psia, to less than 0.01 psid within 180 seconds when initiated by the crew.

3.2.2.7 Verifiable seal leakage paths

Paths through which the atmosphere of any pressurized module might leak to its external environment and which can be verified prior to launch shall have the redundancy and verifiability requirements contained in Table XII.

TABLE XII. Seal redundancy and verifiability requirements		
Seal	Redundancy and verifiability requirements [2,3,4]	
	D <= 6.0 inches	D > 6.0 inches
Feed-through connections [1]	A	B
Rotary	A	B
Windows	A	B
Hatches/Doors	A	B
Berthing/Mechanisms	A	B

Notes:
(1) Includes valves, gages, transducers, etc.
(2) D = Major diameter of the seal.
(3) A = Interface shall have two seals. The assembly shall be verifiable prior to launch.
(4) B = Interface shall have two seals. Each seal shall be verifiable prior to launch and on orbit.

3.2.2.8 Non-verifiable seal leakage paths

The leak path between the common berthing mechanism halves which cannot be verified prior to launch shall have three seals. Each seal shall be verifiable. [Lab PIDS 3.2.2.19]

3.2.2.9 Capability: Support station ingress

The USOS shall support the controlled, tethered entry into the on-orbit Space Station from space by a crew member in an EMU. The USOS shall support contaminant detection and decontamination of the crew and their support equipment for the following types of contamination:

Contamination	Minimum Detection Level (mg/m3)
Hydrazine	0.04
Monomethylhydrazine	0.04
Dimethylhydrazine	0.04
Nitrogen dioxide	2.19
Ammonia	5.0

3.2.2.10 Depressurization and Repressurization for EVA

3.2.2.10.1 Provide repressurization for ingress

Following an EVA when only the Crewlock is at vacuum, the Crewlock shall reach 5.0 psia total pressure within the first 20 seconds of repressurization. When both Airlock chambers are at vacuum, the Airlock shall reach 5.0 psia total pressure within the first 60 seconds of repressurization. The maximum emergency repress rate for the AIrlock shall not exceed 1 psi per second. During an emergency repressurization following an EVA when only the crewlock is at vacuum, both Airlock chambers shall equalize with the USOS to within 0.01 psid within 80 seconds. During an emergency repressurization when both Airlock chambers are at vacuum, the Airlock shall equalize with the USOS within 150 seconds. [USOS 3.7.15.3.95]

3.2.2.10.2 Support station ingress

The USOS shall support the repressurization for a crewmember from vacuum to Space Station atmosphere at a nominal rate of 0.05 psi per second.

3.2.2.10.3 Support station egress

The USOS shall support the controlled, tethered exit from the on-orbit Space Station to space by suited crew members. The USOS shall support depressurization for a crew member from the on-orbit Space Station atmosphere to vacuum at a nominal depressurization rate of 0.05 psi per second. [SSP 41000B 3.7.1.3.26.2]

3.2.2.10.4 Provide depressurization for egress

The Crewlock shall allow depressurization from 14.7 psia to 3.0psia within 12 minutes (maximum). The nominal depress rate for the crewlock shall not exceed 0.05 psi per second. [USOS 3.7.15.3.91]

3.2.2.11 Monitor Oxygen partial pressure

The purpose of this function is to measure the oxygen partial pressure of the <END ITEM> atmosphere for control purposes.

The <END ITEM> shall monitor oxygen partial pressure in the range of 0 to 5.8 psia with an accuracy of +/-2% of full scale. The <END ITEM> shall receive an atmosphere sample from adjacent elements in accordance with SSP 41141, Atmospheric Sampling and SSP 41143, Atmospheric Sampling.

3.2.2.12 Monitor atmosphere temperature

The purpose of this function is to measure the temperature of the <END ITEM> atmosphere for temperature control purposes.

The <END ITEM> shall monitor atmosphere temperature over the range of 60 degrees F to 90 degrees F with an accuracy of +/- 1 degree F.

3.2.2.13 Detect hazardous atmosphere

The purpose of this function is to detect a hazardous atmosphere.

The <END ITEM> shall detect combustion products over the ranges specified in Table IV.

TABLE IV. Combustion product detection

Compound	Range (ppm)
Carbon Monoxide (CO)	5 to 400
Hydrogen Chloride (HCL)	1 to 100
Hydrogen Cyanide (HCN)	1 to 100
Hydrogen Fluoride (HF)/ Carbonyl Fluoride (COF_2)	1 to 100

3.2.2.14 Recover from hazardous atmosphere

The purpose of this function is to provide safe atmosphere restoration and system reconfiguration as necessary.

The <END ITEM> shall repressurize the <END ITEM> atmosphere from space vacuum to a total pressure of 13.9 to 14.9 psia and an oxygen partial pressure of 2.83 to 3.35 psia within 75 hours.

3.2.2.15

The <END ITEM> shall provide a 15 minute supply of portable emergency oxygen per crewmember for two crewmembers.

3.2.2.16 Monitor carbon dioxide

The purpose of this function is to monitor the level of carbon dioxide in the International Space Station atmosphere.

The <END ITEM> shall monitor the <END ITEM> atmosphere of carbon dioxide partial pressure over a range of 0 to 15 mmHg with an accuracy of +/- 1 percent of full scale.

3.2.2.17 Remove gaseous contaminants

The purpose of this function is to maintain contaminant concentrations in the atmosphere below acceptable limits.

The HAB A shall support station level requirements to control contaminant concentrations in the atmosphere to levels less than or equal to the Spacecraft Maximum Allowable Concentration (SMAC) levels specified in Table IX and Table IX-A. For those compounds listed in Table IX-A, the control will be based on the generation rates listed in Table IX, a total internal mass of 75,000 kg, and a metabolic equivalent of 5.25 men (4 crew plus 1.25 MEQ for animals).

TABLE IX. Spacecraft maximum allowable concentrations

		Potential Exposure Period				
Chemical		1 h	24 h	7 d	30 d	180 d
ACETALDEHYDE	MG/M^3	20	10	4	4	4
ACROLEIN	MG/M^3	0.2	0.08	0.03	0.03	0.03
AMMONIA	MG/M^3	20	14	7	7	7
CARBON DIOXIDE	MM/HG	10	10	5.3	5.3	5.3
CARBON MONOXIDE	MG/M^3	60	20	10	10	10
1,2-DICHLOROETHANE	MG/M^3	2	2	2	2	1
2-ETHOXYETHANOL	MG/M^3	40	40	3	2	0.3
FORMALDEHYDE	MG/M^3	0.5	0.12	0.05	0.05	0.05
FREON 113	MG/M^3	400	400	400	400	400
HYDRAZINE	MG/M^3	5	0.4	0.05	0.03	0.005
HYDROGEN	MG/M^3	340	340	340	340	340
INDOLE	MG/M^3	5	1.5	0.25	0.25	0.25
MERCURY	MG/M^3	0.1	0.02	0.01	0.01	0.01
METHANE	MG/M^3	3800	3800	3800	3800	3800
METHANOL	MG/M^3	40	13	9	9	9
METHYL ETHYL KETONE	MG/M^3	150	150	30	30	30
METHYL HYDRAZINE	MG/M^3	0.004	0.004	0.004	0.004	0.004
DICHLOROMETHANE	MG/M^3	350	120	50	20	10

OCTAMETHYLTRISILOXANE	MG/M^3	4000	2000	1000	200	40
2-PROPANOL	MG/M^3	1000	240	150	150	150
TOLUENE	MG/M^3	60	60	60	60	60
TRICHLOROETHYLENE	MG/M^3	270	60	50	20	10
TRIMETHYLSILANOL	MG/M^3	600	70	40	40	40
XYLENE	MG/M^3	430	430	220	220	220

TABLE IX-A. Spacecraft trace contaminant generation rates and SMACs

	COMMON NAME	IUPAC NAME	MOLAR MASS g/mol	SMAC mg/m3	EQUIPMENT GEN RATE mg/day*kg	METABOLIC GEN RATE mg/man*day
	ALCOHOLS					
1	Methyl alcohol	Methanol	32.04	9.00	1.27E-03	1.50E+00
2	Ethyl alcohol	Ethanol	46.07	94.00	7.85E-03	4.00E+00
3	Allyl alcohol	2-propen-1-ol	58.08	1.00	2.35E-06	0.00E+00
4	Isopropyl alcohol	2-propanol	60.09	150.00	3.99E-03	0.00E+00
5	Propyl alcohol	n-propanol	60.09	98.30	2.41E-04	0.00E+00
6	Ethylene glycol	1,2-ethanediol	62.07	127.00	6.03E-06	0.00E+00
7	2-butanol	2-butanol	74.12	121.00	9.63E-06	0.00E+00
8	Isobutyl alcohol	2-methyl-1-propanol	74.12	121.00	8.46E-04	1.20E+00
9	tert-butyl alcohol	2-methyl-2-propanol	74.12	121.00	7.38E-05	0.00E+00
10	Butyl alcohol	n-butanol	74.12	121.00	4.71E-03	1.33E+00
11	n-amyl alcohol	n-pentanol	88.15	126.00	1.62E-04	0.00E+00
12	Phenol	Phenol	94.11	7.70	4.83E-04	0.00E+00
13	Hexahydrophenol	Cyclohexanol	100.16	123.00	7.56E-04	0.00E+00
14	2-hexanol	2-hexanol	102.18	167.00	2.48E-06	0.00E+00
	ALDEHYDES					
15	Formaldehyde	Methanal	30.03	0.05	4.40E-08	0.00E+00
16	Acetaldehyde	Ethanal	44.05	4.00	1.09E-04	9.00E-02
17	Acrolein	2-propenal	56.06	0.03	3.46E-06	0.00E+00
18	Propionaldehyde	Propanal	58.08	95.00	3.19E-04	0.00E+00
19	n-butylaldehyde	Butanal	72.10	118.00	8.59E-04	0.00E+00
20	valeraldehyde	Pentanal	86.13	106.00	7.84E-05	8.30E-01
21	benzenecarbonal	Benzaldehyde	106.12	173.00	1.99E-05	0.00E+00
	AROMATIC HYDROCARBONS					

22	Benzene	Benzene	78.11	0.32	2.51E-05	0.00E+00
23	Toluene	Methylbenzene	98.13	60.00	1.98E-03	0.00E+00
24	Styrene	Vinylbenzene	104.14	42.60	3.13E-05	0.00E+00
25	o-xylene	1,2-dimethylbenzene	106.16	86.80	5.56E-04	0.00E+00
26	m-xylene	1,3-dimethylbenzene	106.16	86.80	2.03E-03	0.00E+00
27	p-xylene	1,4-dimethylbenzene	106.16	86.80	1.08E-03	0.00E+00
28	Ethylbenzene	Ethylbenzene	106.16	86.80	1.50E-04	0.00E+00
29	alpha-methylstyrene	alpha-methylstyrene	118.18	145.00	1.67E-07	0.00E+00
30	Pseudocumene	1,2,4-trimethylbenzene	120.20	15.00	4.49E-05	0.00E+00
31	Mesitylene	1,3,5-trimethylbenzene	120.20	15.00	3.63E-06	0.00E+00
32	1-ethyl-2-methylbenzene	1-ethyl-2-methylbenzene	120.20	25.00	4.88E-06	0.00E+00
33	Cumene	Isopropylbenzene	120.20	73.70	1.40E-05	0.00E+00
34	Propylbenzene	Propylbenzene	120.20	49.10	2.15E-04	0.00E+00
	ESTERS					
35	ethyl formate	Ethyl formate	74.08	90.90	4.51E-06	0.00E+00
36	methyl acetate	Methyl acetate	74.08	121.00	1.41E-04	0.00E+00
37	ethyl acetate	Ethyl acetate	88.11	180.00	2.97E-04	0.00E+00
38	methyl methacrylate	Methyl methacrylate	100.12	102.00	1.30E-04	0.00E+00
39	isopropyl acetate	Isopropyl acetate	102.13	209.00	5.81E-06	0.00E+00
40	propyl acetate	Propyl acetate	102.13	167.00	3.38E-04	0.00E+00
41	butyl acetate	Butyl acetate	116.16	190.00	7.46E-04	0.00E+00
42	isobutyl acetate	Isobutyl acetate	116.16	190.00	1.52E-04	0.00E+00
43	ethyl lactate	Ethyl lactate	118.13	193.00	3.64E-06	0.00E+00
44	n-amyl acetate	n-amyl acetate	130.18	160.00	4.78E-05	0.00E+00
45	cellosolve acetate	2-ethoxyethyl acetate	132.16	162.00	7.46E-04	0.00E+00
	ETHERS					
46	Furan	1,4-epoxy-1,3-butadiene	68.07	0.11	1.84E-06	0.00E+00
47	Tetrahydrofuran	1,4-epoxybutane	72.11	118.00	6.93E-05	0.00E+00
48	Ether	Diethyl ether	74.12	242.00	8.90E-05	0.00E+00
49	sylvan	2-methylfuran	82.10	0.13	3.46E-06	0.00E+00
50	ethyl cellosolve	2-ethoxyethanol	90.12	0.30	6.01E-04	0.00E+00
	CHLOROCARBONS					

51	Methyl chloride	Chloromethane	50.49	41.30	6.76E-06	0.00E+00
52	Vinyl chloride	Chloroethene	62.50	0.26	1.46E-06	0.00E+00
53	Ethyl chloride	Chloroethane	64.52	263.70	8.99E-08	0.00E+00
54	Methylene chloride	Dichloromethane	84.93	10.00	2.15E-03	0.00E+00
55	dichloroethene	1,1-dichloroethene	96.95	7.90	5.64E-07	0.00E+00
56	Ethylene dichloride	1,2-dichloroethane	98.97	1.00	7.74E-05	0.00E+00
57	Chlorobenzene	Chlorobenzene	112.56	46.00	1.54E-03	0.00E+00
58	propylene chloride	1,2-dichloropropane	112.99	42.20	7.42E-06	0.00E+00
59	Chloroform	Trichloromethane	119.38	4.90	1.76E-05	0.00E+00
60	Trichloroethylene	Trichloroethylene	131.39	10.00	8.62E-05	0.00E+00
61	Methyl chloroform	1,1,1-trichloroethane	133.41	164.00	6.72E-04	0.00E+00
62	Vinyl trichloride	1,1,2-trichloroethane	133.41	5.50	8.24E-08	0.00E+00
63	dichorobenzene	1,2-dichlorobenzene	147.01	30.00	6.33E-06	0.00E+00
64	Carbon tetrachloride	Tetrachloromethane	153.82	13.00	9.60E-06	0.00E+00
65	Tetrachloroethylene	Tetrachloroethene	165.83	34.00	7.28E-04	0.00E+00
	CHLOROFLUOROCARBONS					
66	Freon 22	Chlorodifluoromethane	86.47	353.60	5.75E-05	0.00E+00
67	Freon 21	Dichlorofluoromethane	102.90	21.00	6.36E-07	0.00E+00
68	chlorotrifluoroethane	1-chloro-1,2,2-trifluoroethane	118.50	484.50	4.88E-06	0.00E+00
69	Freon 12	Dichlorodifluoromethane	120.91	494.40	1.35E-05	0.00E+00
70	dichorodifluoroethene	1,2-dichloro-1,2-difluoroethene	132.93	136.00	1.89E-06	0.00E+00
71	Freon 11	Trichlorofluoromethane	137.40	561.80	1.41E-03	0.00E+00
72	Halon 1301	Bromotrifluoromethane	148.90	608.80	2.61E-04	0.00E+00
73	Freon 114	1,1-dichloro-1,2,2,2-tetrafluoroethane	170.92	702.90	2.62E-05	0.00E+00
74	Freon 113	1,1,2-trichloro-1,2,2-trifluoroethane	187.40	400.00	1.89E-02	0.00E+00

75	Freon 112	1,1,2,2-tetrachloro-1,2-difluoroethane	204.00	834.20	3.33E-05	0.00E+00
	HYROCARBONS					
76	Methane	Methane	16.04	3800.00	6.39E-04	1.60E+02
77	Ethylene	Ethene	28.05	344.10	2.27E-07	0.00E+00
78	Ethane	Ethane	30.07	1230.00	1.17E-06	0.00E+00
79	Propylene	Propene	42.08	860.30	2.56E-06	0.00E+00
80	Propane	Propane	44.09	901.40	9.21E-07	0.00E+00
81	Vinylethylene	1,3-butadiene	54.09	221.20	2.66E-06	0.00E+00
82	Ethylethylene	1-butene	56.10	458.00	8.03E-05	0.00E+00
83	Isobutane	2-methylpropane	58.12	237.60	1.10E-05	0.00E+00
84	Butane	Butane	58.12	237.60	5.13E-06	0.00E+00
85	Propylethylene	1-pentene	70.13	186.00	2.20E-08	0.00E+00
86	Isopentane	2-methylbutane	72.15	295.00	1.80E-06	0.00E+00
87	Pentane	Pentane	72.15	590.00	9.54E-05	0.00E+00
88	hexamethylene	Cyclohexane	84.16	206.00	3.79E-04	0.00E+00
89	methylpentamethylene	Methylcyclopentane	84.16	51.60	2.97E-05	0.00E+00
90	Neohexane	2,2-dimethylbutane	86.17	88.10	1.67E-06	0.00E+00
91	Diethylmethylmethane	3-methylpentane	86.18	1762.00	5.97E-06	0.00E+00
92	Hexane	Hexane	86.18	176.00	6.95E-05	0.00E+00
93	1-heptylene	1-heptene	98.18	201.00	1.10E-08	0.00E+00
94	Hexahydrotoluene	Methylcyclohexane	98.18	60.20	6.09E-05	0.00E+00
95	Heptane	Heptane	100.21	205.00	5.59E-05	0.00E+00
96	Dimethylcyclohexane	1,1-dimethylcyclohexane	112.22	115.00	2.61E-05	0.00E+00
97	trans-1,2-dimethylhexamethylene	trans-1,2-dimethylcyclohexane	112.22	115.00	5.23E-05	0.00E+00
98	octane	Octane	114.23	350.00	1.61E-05	0.00E+00
99	nonane	Nonane	128.26	315.00	7.35E-06	0.00E+00
100	citrene (limonene)	4-isopropenyl-1-Mecyclohexene	136.23	557.00	3.58E-06	0.00E+00

101	Decane	Decane	142.28	223.00	2.78E-05	0.00E+00
102	Hendecane	Undecane	156.31	319.00	2.51E-05	0.00E+00
103	Dodecane	Dodecane	170.34	278.00	6.91E-07	0.00E+00
	KETONES					
104	Acetone	2-propanone	58.08	712.50	3.62E-03	2.00E-01
105	Methyl ethyl ketone	2-butanone	72.11	30.00	6.01E-03	0.00E+00
106	Methyl propyl ketone	2-pentanone	86.13	70.40	4.03E-06	0.00E+00
107	Methyl isopropyl ketone	3-methyl-2-butanone	86.13	70.40	3.11E-05	0.00E+00
108	Mesityl oxide (methyl isobutenyl ketone)	4-methyl-3-penten-2-one	98.14	40.10	1.91E-04	0.00E+00
109	cyclohexanone (pimelic ketone)	Cyclohexanone	98.14	60.20	6.62E-04	0.00E+00
110	Methyl isobutyl ketone	4-methyl-2-pentanone	100.16	82.00	1.41E-03	0.00E+00
111	Phenyl methyl ketone	acetophenone	120.14	245.00	5.66E-07	0.00E+00
112	Methyl hexyl ketone	2-octanone	128.21	105.00	1.65E-07	0.00E+00
113	Diisobutyl ketone	2,6-dimethyl-4-heptanone	142.20	58.10	3.34E-06	0.00E+00
	MERCAPTANS and SULFIDES					
114	hydrogen sulfide	Hydrogen sulfide	34.08	2.80	0.00E+00	9.00E-02
115	Carbon oxisulfide	Carbonyl sulfide	60.07	12.00	6.05E-06	0.00E+00
116	Methyl sulfide	Dimethyl sulfide	62.14	2.50	1.88E-07	0.00E+00
117	carbon disulfide	Carbon disulfide	76.14	16.00	3.23E-05	0.00E+00
	ORGANIC ACIDS					
118	Acetic acid	Ethanoic acid	60.05	7.40	1.42E-06	0.00E+00
	ORGANIC NITROGENS					
119	Acetonitrile	Methyl cyanide	41.05	6.70	1.70E-08	0.00E+00
120	Indole	2,3-benzopyrrole	117.15	0.25	0.00E+00	6.25E+00
	MISCELLANEOUS					
121	hydrogen	Hydrogen	2.02	340.00	5.91E-06	2.60E+01

122	ammonia	Ammonia	17.00	7.00	8.46E-05	3.21E+02
123	carbon monoxide	Carbon monoxide	28.01	10.00	2.03E-03	2.30E+01
124	trimethylsilanol	Trimethylsilanol	90.21	40.00	1.69E-04	0.00E+00
125	hexamethylcyclotrioxosilane	Hexamethylcyclotrisiloxane	222.40	227.00	1.62E-04	0.00E+00
126	octamethyltrioxosilane	Octamethyltrisiloxane	236.54	40.00	2.11E-04	0.00E+00

3.2.2.18 Remove airborne microbes

The purpose of this function is to remove airborne microbes from the <End Item> atmosphere.

The <End Item> shall limit the daily average airborne microbes in the <End Item> atmosphere to 1000 Colony Forming Units (CFU) per cubic meter.

3.2.2.19 Monitor airborne microbes

The purpose of this function is to monitor the level of airborne microbes in the <END ITEM> atmosphere. The <END ITEM> shall monitor the <END ITEM> atmosphere for bacteria and fungi: with a sampling volume of 1 to 1000 liters of atmosphere. The <END ITEM> shall monitor bacteria with a sampling range of 0 to 1,125 colony forming units (CFU) per cubic meter and fungi with a sampling range of 1,250 CFU per cubic meter.

3.2.2.20 Mode: Assured safe crew return

This mode provides mitigation capability for life threatening illness, unrecoverable loss of station habitability, or extended problem requiring resupply/servicing which is prevented from occurring due to launch problems. This mode consists of the actions/operations/functions necessary to safely populate the Assured Crew Return Vehicle (ACRV), separate and return the ACRV to earth, and egress the ACRV upon recovery on the ground. The mode consists of the capabilities as shown in SSP 41000, Rev. B, Table VIII, and the following unique capability.

3.2.3 Caution and Warning

3.2.3.1 Annunciate alarms

The purpose of this function is to provide audible and visual alarms to the crew. The <END ITEM> shall annunciate Class 1, 2 and 3 audio and visual alarms in accordance with SSP 50005, Caution and Warning Displays. The <END ITEM> shall provide the facilities to allow on-orbit operators to acknowledge alarms. This requirment shall be located within each segment and may

not apply to each end item (e.g. MPLM) if capability is provided through another end item or segment.

3.2.4 Fault Detection Isolation and Recovery

3.2.4.1 Reserved

3.2.4.2 Isolate to the recovery level

The USL shall automatically isolate detected failures to the functional recovery level for those functions requiring automatic isolation, identified in SSP 41000, Rev. B, Table II, column 3.

3.2.4.3 Isolate hazard

The <End Item> shall isolate hazards, that exhibit a time to catastrophic or critical effect of less than 24 hours, to the on-orbit safing level.

3.2.4.4 Assess functional data

The <End Item> shall automatically assess the collected data to detect failures of those functions requiring automatic assessment and to detect hazards that may exhibit a time to catastrophic or critical effect of less than 24 hours.

3.2.4.5 Manual FDIR

The following categories of equipment shall utilize crew interaction or crew observation for manual failure detection, isolation, annunciation, and recovery:

a. Human/equipment interface such as visual display devices, cursor control devices, manual input devices.

b. General and specialized lighting.

c. Visual and aural caution and warning devices such as warning panel lamps/lights, speakers and volume controls.

d. Structural, mechanical, electro-mechanical, and electrical equipment that have no interconnection for data collection and transmission to the core computational data network such as fluid, power, and data lines, structure and manually operated equipment.

e. One-time use equipment that has manual redundancy (crew intervention upon failure of automatic function) and is not intended to be maintained on-orbit during the life of the program such as bolt motor controllers for assembly operations.

3.2.4.6 Manual control of FDIR

The <End Item> shall provide for manual control of automatic detection, isolation, and recovery control processes.

3.2.4.7 Collect function status data

The purpose of this function is to collect applicable data for assessment of functional health, out of tolerance conditions, functional performance, functional failures, and other status data per SSP 50038.

3.2.4.8

The <END ITEM> shall obtain data identifying out-of-tolerance conditions, functional failures, and data describing functional operation. The <END ITEM> shall make available, to automatic capabilities and to operators on demand in accordance with the paragraph ”S/W Functional Interfaces” of SSP 41143, SSP 42011, and SSP 41141, all generated Built In Test (BIT) data and results of process execution or effector manipulation per SSP 50038.

3.2.4.9 Condition function status data

The purpose of this function is to condition data into a usable form. This data is then available upon demand by other capabilities or operators.

The <END ITEM> shall condition functional data for identified users. The <END ITEM> shall make available, to automatic capabilities and to operators on demand in accordance with the paragraph ”S/W Functional Interfaces” of SSP 41143, SSP 42011, and SSP 41141, all conditioned BIT data per SSP 50038, see paragraph 3.2.4.10.11.

3.2.5 Lighting

3.2.5.1 Illuminate general area

The purpose of this function is to illuminate general areas of the USL.

The USL shall illuminate general activity areas at a minimum of 10 foot-candle (108 lux) of white light. The USL shall illuminate the passageways at a minimum of 5 foot candles (54 lux) of white light.

3.2.5.2 Illuminate emergency egress area

The purpose of this function is to illuminate the emergency egress areas of the <END ITEM>.

The <END ITEM> shall illuminate the emergency egress area at a minimum of 0.05 foot candle (0.5 lux) for pressurized module exits. The <END ITEM> shall illuminate the emergency controls at a minimum of 0.01 foot candle (0.108) lux for emergency controls.

3.2.5.3 Control emergency egress lighting

The purpose of this function is to control the automatic turn on of the emergency egress lighting when an emergency is recognized.

3.2.6 Noise

3.2.6.1 Acoustic emission limits

The integrated acoustic environment in habitable areas in the <End Item> shall not exceed the US NC-50 criterion during normal operating conditions when, averaged over a minimum of 10 second time interval. In areas where crewmembers must communicate by voice, the reveberation time shall not exceed 0.5 +/- 0.1 seconds at 1000 Hz.

3.2.7 Radiation

3.2.7.1 Ionizing radiation crew limits

The design of the USL shall limit the ionizing radiation dose in habital volumes to 40 rem (BFO) per year.

3.2.7.2 Ionizing radiation emission limits

Ionizing radiation emissions from USL equipment shall not exceed 2 millirads silicon per day, one centimeter from any surface.

3.2.7.3 Support radiation exposure monitoring

The <End Item> shall monitor crew environment exposure to radiation.

3.2.7.4 Reserved

3.2.7.5 Meteoroids and orbital debris (M/OD)

The <End Item> M/OD critical items shall meet the requirements specified herein when exposed to the M/OD environments defined in SSP 30425, Meteoroids and Orbital Debris. Parameters of International Space Station M/OD environments definition are given in Table IX.

TABLE IX. Parameters for M/OD environments definition.

Altitude	215 nautical miles (400 km)
Orbital inclination	51.6 degrees
Space Station attitude	LVLH 10% of the time (Orbiter attached) TEA 90% of the time (Orbiter not attached)
Solar flux	70×10^4 Jansky ($F_{10.7} = 70$)
Orbital debris density(1)	2.8 gm/cm^3
Maximum debris diameter	20 cm

Note:

(1) For M/OD critical items only

3.2.7.6 Probability of no penetration

The Space Station shall have a 0.81 (minimum) combined Probability of No Penetration (PNP) of M/OD critical items (See Appendix B) in the M/OD environment defined in 3.2.6.1.8 [of SSP 41000B], for 10 years from First Element Launch (FEL). [SSP 41000B, 3.3.12.1.1]

3.2.7.7

The <End Item> shall have provisions for M/OD protection augmentation.

3.2.7.8 Environmental conditions

The <End Item> shall satisfy the requirements of this specification when subjected to the environmental conditions for the environments and environmental phases specified below.

3.2.7.9 Electromagnetic Radiation

3.2.7.10 EMC

The shall meet the requirements specified in SSP 30243

3.2.7.11 EMI

Electrical and electronic equipment shall meet requirements in SSP 30237

3.2 7.12 Electrical Grounding

Electrical Grounding shall be in acordance with SSP 30240

3.2.7.13 Electrical Bonding

Electrical Bonding shall be in acordance with SSP 30245

3.2.7.14 Plasma

The <End Item> shall meet the performance and design requirements specified herein when exposed to the natural plasma environment as specified in SSP 30425, Section 5 and the induced environment as specified in SSP 30420, section 3.3. The difference between the <End Item> structure floating potential and the local plasma potential does not exceed +/-40 volts.

3.2.7.15 Ionizing radiation

The <End Item> shall meet specified performance when exposed to the radiation dose environment as specified in SSP 30512. A radiation dose design margin of two shall be applied.

3.2.7.16 Electrostatic Discharge (ESD)

The <End Item> shall meet the requirements as specified in SSP 30243.

3.2.7.17 Corona

The <End Item> shall meet the requirements as specified in SSP 30243.

3.2.7.18 Cable and wire design

<End Item> interconnect and interconnect cable and wire design shall be in accordance with SSP 30242.

3.2.8 Respond to Fire

The USOS shall detect a fire event in locations in accordance with the selection criteria in Figure 24 and in the open cabin volume. The USOS shall isolate a fire event within 30 seconds of detection, including removal of power and forced airflow at the affected location, in locations in accordance with the selection criteria in Figure 24. The USOS shall accommodate Portable Breathing Apparatuses (PBAs) and provide Portable Fire Extinguisher (PFEs). The USOS shall activate a Class I alarm for a detected fire event with event location. The USOS shall visually indicate a fire event at the detection location. The USOS shall prevent forced air circulation between elements within 30 seconds of annunciation of a Class I fire alarm. Fixed fire suppression, where installed, shall complete application of fire suppressant within one minute of initiation. The USOS fire suppression shall reduce the oxygen concentration at the fire event location to less than 10.5 percent within one minute of suppressant discharge. The USOS shall have fixed fire suppression in locations in accordance with the selection criteria in Figure 24. Fixed fire suppression, where installed, shall have remote activation capability. When initiated by the crew or ground, the USOS shall vent the atmosphere of any pressurized volume to space to achieve an oxygen partial pressure less than 1.0 psia within 10 minutes. The USOS shall restore the habitable environment after a fire event. [SSP 41000B, P 3.7.1.3.8.1, CCM 00077]

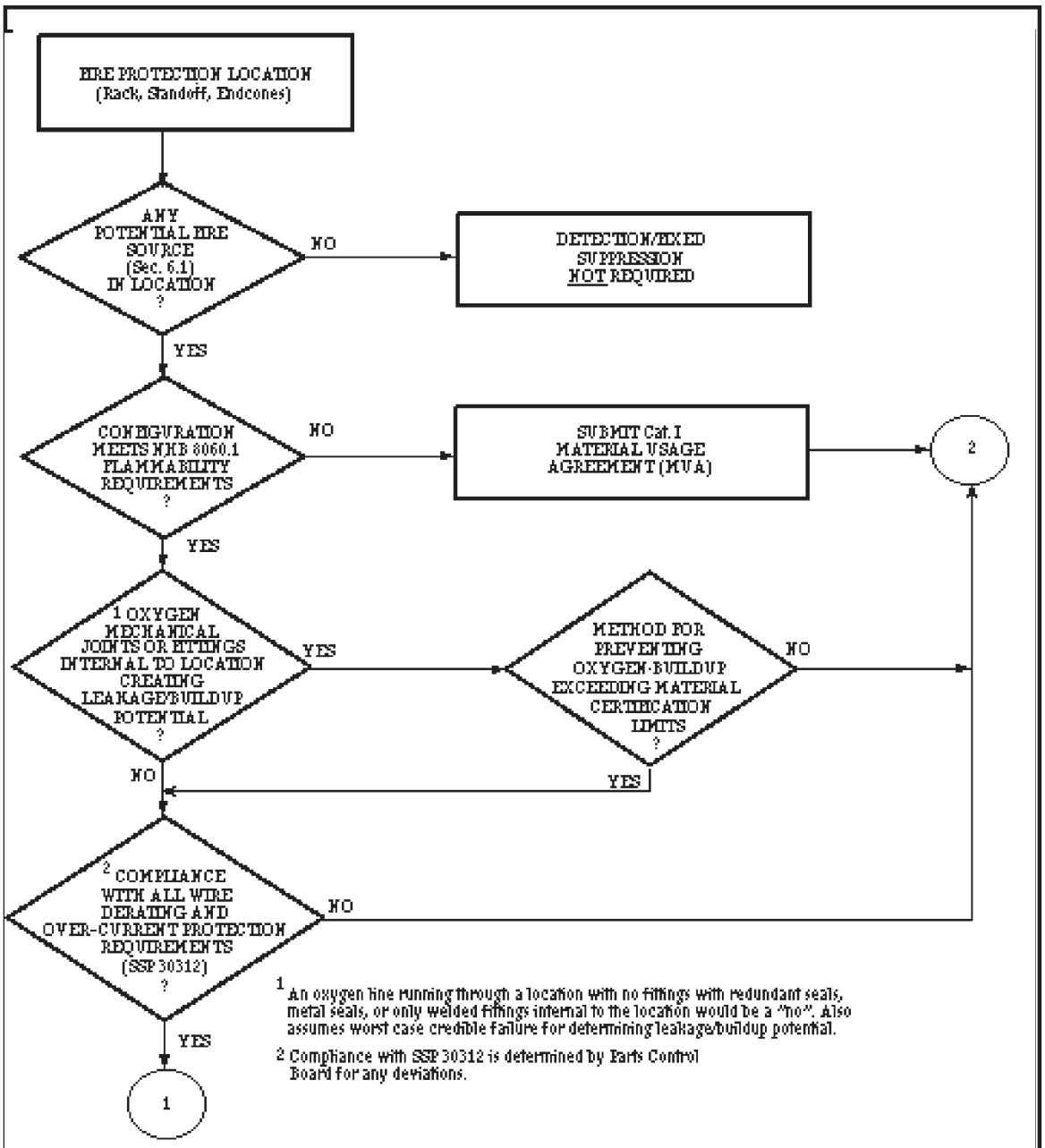
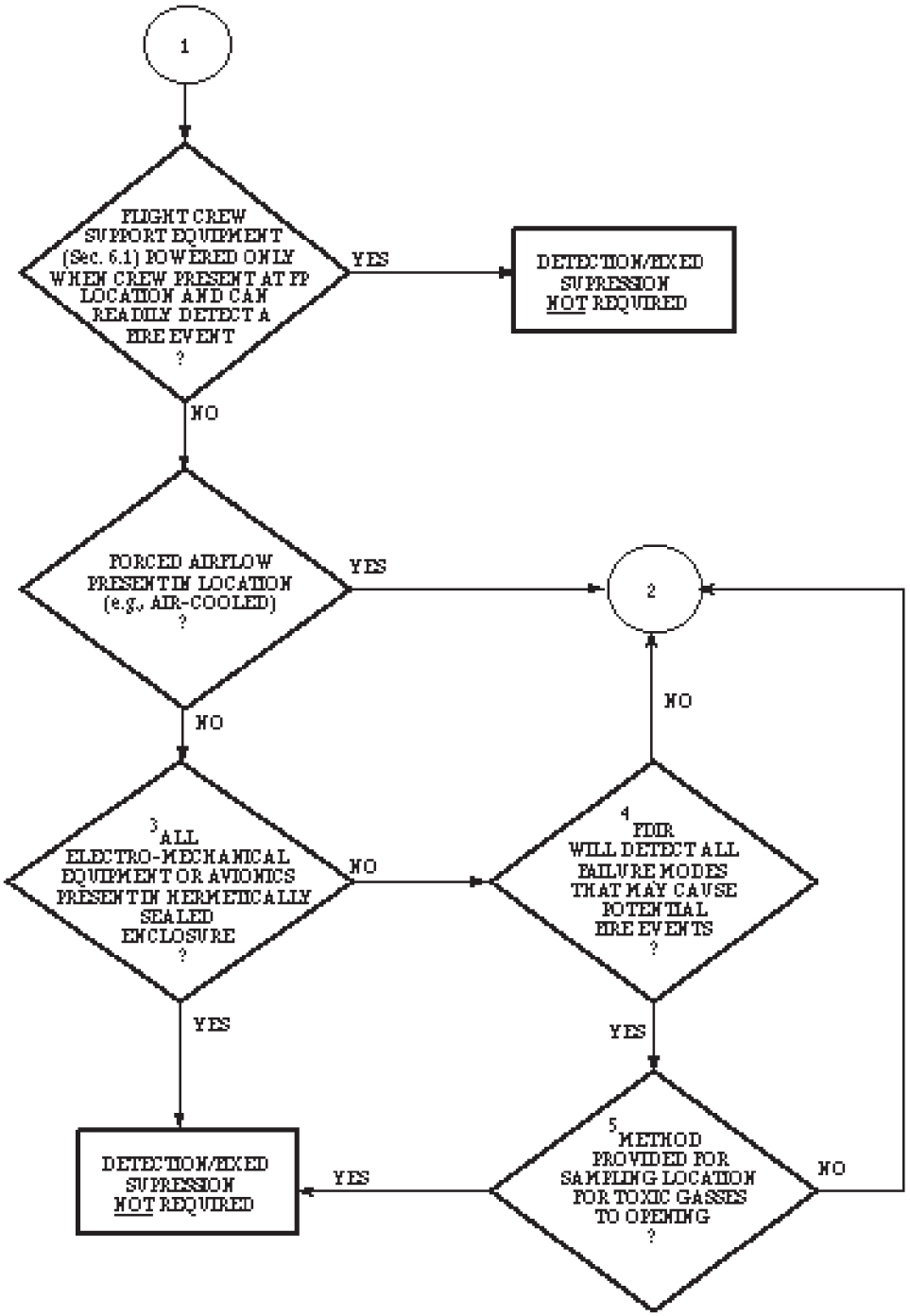


FIGURE 24 Fire protection selection criteria

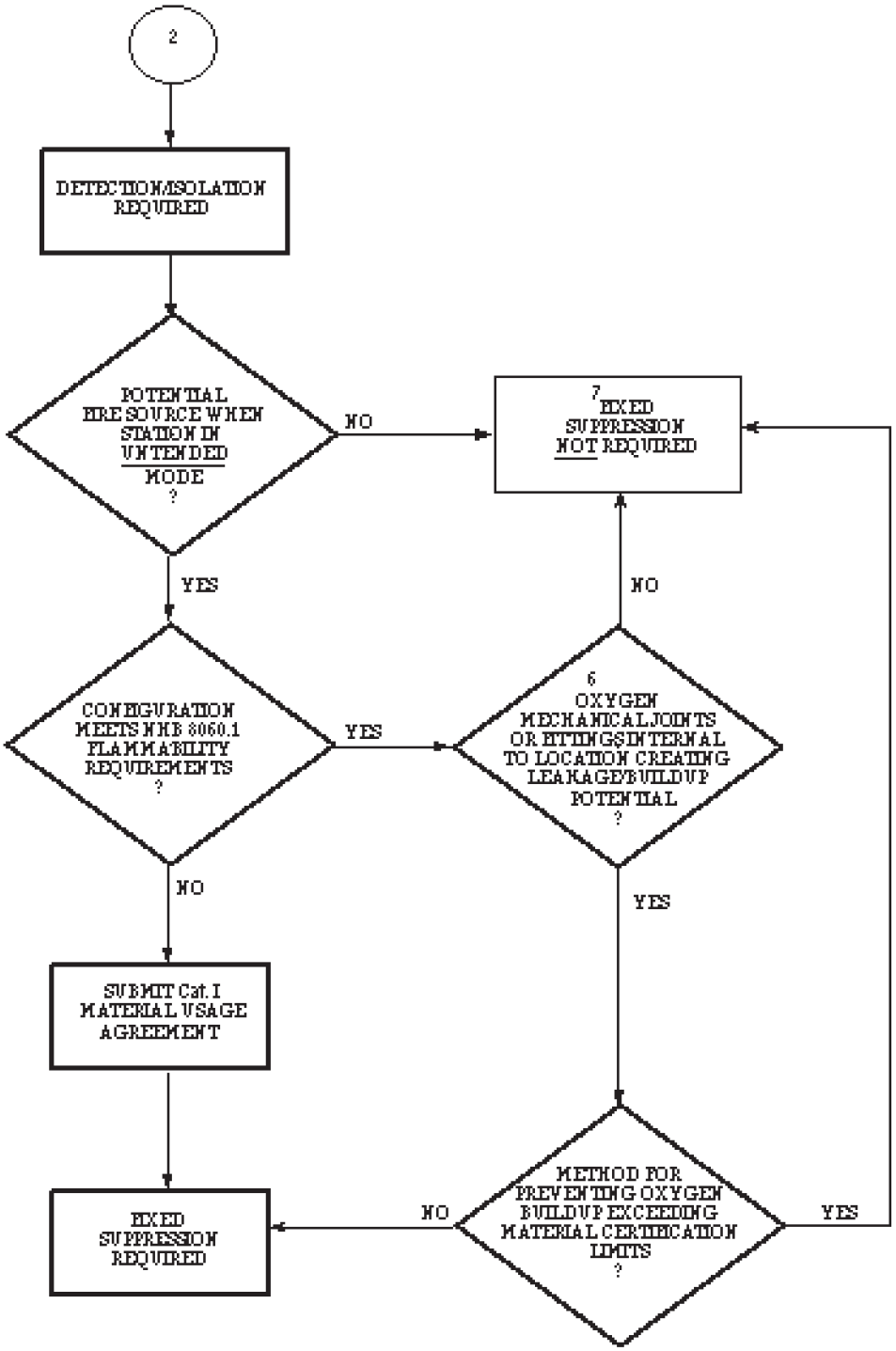


[3] Avionics refers to any electrical equipment or components other than power/data connectors, cables, lines, or wires (e.g., card mounted electronic components). Electro-mechanical equipment refers to any motors, pumps, etc.

[4] FDIR must be sufficient to alert the crew to failure modes of the equipment, not in hermetically sealed enclosures, which could cause a fire event. Notification of loss of function satisfies the FDIR requirement. Electrical equipment and wiring having two upstream devices to detect and isolate overcurrent and short circuit conditions meet the FDIR requirements.

[5] Sampling is intended to allow the crew to avoid opening a location which may contain a buildup of hazardous off gassing. Sampling through a PFE suppression port using the GFE Manual Sampling Equipment satisfies this equipment.

FIGURE 24. Fire protection selection criteria - Continued



6 An oxygen line running through a location with no fittings, fittings with redundant seals, metal seals, or only welded fittings internal to the location would be a "no". Assumes worst case credible failure for determining leakage/buildup potential.

7 Based on capability of crew to perform suppression via Portable Fire Extinguishers (PFE) for locations which will be powered only when station is tended. When the station is untended the material control and no oxygen leakage/buildup potential will prevent a fire from propagating.

FIGURE 24. Fire protection selection criteria - Continued

3.2.9 Materials

3.2.9.1 Materials and processes

Materials and processes shall be selected in accordance with SSP 30233.

3.2.9.2 Fluid leakage

Fluid system leaks shall be isolated and controlled.

3.2.9.3 Used for hazardous fluids

Self-Sealing Quick Disconnects shall be used on components of fluid systems which would create a hazardous condition during on-orbit maintenance.

3.2.10 Structures

3.2.10.1 Structural design requirements

<End Item> structures shall be designed in accordance with SSP 30559 Section 3.0. For the purpose of conducting structural analysis, the service life will be 15 years. For the purpose of conducting meteoroid and debris penetration analysis, the service life will be based on a 10 year on-orbit exposure period. The interface loads are defined in the ICDs defined in 3.1.2.

3.2.10.2 EVA on-orbit induced loads

<End Item> external structure shall support the limit loads induced by an EVA crew member provided in Table XXV. [Lab PIDS 3.3.12.1.3.2]

TABLE XXV. EVA induced loads

DESIGN LIMIT LOAD TYPE	LIMIT LOAD	TYPE OF LOADING	DIRECTION	CATEGORY OF STRUCTURE	APPLICATION COMMENTS
EVA Handrail/Handhold-Primary Translation Path	220 lbf	Quasi-static load applied over 3.0 inch length of handrail or handhold at worst location	Any direction	Handrails, handholds, and supporting structure	This load applied to the primary translation path used by the crewmember to return to the airlock. This path is identified in the EVA Standard ICD.
Handrail/ Handhold-Secondary Translation Path	187 lbf	Quasi-static load applied over 3.0 inch length of handrail or handhold at worst location	Any direction	Handrails, handholds, and supporting structure	This load applied to the secondary translation path.
Crew Tether Attach	200lbf	Quasi-static load applied to crew Tether Loop Attachment	Any direction	Crew tether loops/handrail tether point, attach hardware, and support structure	
EVA Kick-Off, Push-Off Force of Tethered Crew Member	200lbf	Quasi-static concentrated load over a 3.0 inch diameter circular area at worst location	Perpendicular to and directed toward surface	All primary and secondary structure inside or near (within 24 inch) a translation path or worksite	This maximum kick-off or push-load applies where the crewmember is using the hardware to provide a reaction point during translation
Inadvertent kick, bump	125 lbf	Quasi-static, concentrated load over	Any direction	Secondary structure near (within 24 in.) translation path	This is an accidental impact. It should be applied to

		a 0.5 inch diameter circular area		or worksite	hardware near (within 24 inches) translation paths and worksites.
Force Application (EVA Handling Load)	45 lbf (35 in-lbf for connector panels for mate/ demate of connector)	Quasi-static concentrated load over a 1.25 inch radius circular area.	Any direction	ORUs and non-structural closures and covers (including shields, cables, cable connector brackets, cable connector panels, cable clamps)	This load can be applied anytime to any hardware by the EVA crewmember when in a foot restraint. All hardware must be designed to this load as a minimum. This force would be applied by the palm of the glove, tip of a boot, or knee.
EVA load for design of PFR supporting structure	274 lbf force; 4200 in-lb moment	Quasi-static load applied at PFR socket to structure interface	Force in any direction; moment about any axis	All structure on which a foot restraint is attached	Force and moment applied simultaneously.
EVA tool tether attach point	75 lbf	Concentrated load-pull (tension)	Any direction	Any structures supporting tool tether attach points	
Hatches	187 lbf	Quasi-static concentrated load over a 3.0 inch diameter circular area at worst location	Any direction	Hatches	
Tool Impact	125 lbf	Concentrated load on a 0.06 inch radius circular area	Any direction	Windows and exposed glass	

Note:

EVA on-orbit induced loads for inadvertent kick and kick-off, push-off loads do not apply to hardware or worksites which are assembled or maintained using robotic systems (crewmember restrained on SRMS or SSRMS).

3.2.10.3 Margin(s) of Safety

International Space Station flight hardware structure shall have +0.00 or positive Margin(s) of Safety (MS) for all yield and ultimate design load conditions

3.2.10.4 End-of-life decommissioning and disposal

The International Space Station shall allow for safe disposal of the on-orbit International Space Station at the end of its useful life.

3.2.10.5 Negative Differential Pressure

Negative pressure differential on primary payload structure shall use a factor of safety of 2.0 if certification for these loads is by analysis only.

3.2.10.6 IVA crew load requirements

Equipment exposed to the translation path shall withstand a design load of 556N (125lbf) and an ultimate load of 778 N (175lbf)

3.2.10.7 External limit loads

External components of <segment hardware> which shall have a crew or crew actuated tool interfaces shall be operable by the loads defined in Table XXVII Miscellaneous crew activation limit loads.

TABLE XXVII. Miscellaneous crew activation load limits			
Crew System	Type of Load	Limit Load	Direction of Load
Tool design - Fine motor activity w/ gloved hand	Concentrated load	< 5 lbs force < 40 in-oz torque	Any direction
- Gross motor skills with low loads	Concentrated load	< 20 lb force	Any direction
EVA mechanical resistive force	Concentrated load	> 3.5 lb	Any direction
EVA hatches and doors	Concentrated load	< 25 lb (latch mechanism) < 45 lb (opening the hatch) < 45 lb (closing the hatch)	Any direction
EVA connectors	Concentrated load	<35 in-lb (mate/demate)	Torque
Drawer movement (EVA)	Concentrated load	< 35 lb (opening/closing) < 35 lb (remove/install)	
Mounting hardware (install/remove) (EVA)	Concentrated load	< 35 lb	
High Torque Fasteners (without torque reaction I/F)	Concentrated load	<25 ft-lb	Torque
High Torque Fasteners (with torque reaction I/F)	Concentrated load	<100 ft-lb	Torque

3.2.10.8 IVA Induced Loads

<End Item> internal structure shall meet requirements specified herein when exposed to IVA crew induced loading as defined in SSP 50005.

3.2.10.9 Fracture Control

<End Item> structure shall be designed for fracture control in accordance with SSP 30558.

3.2.10.10 Glass, window, and ceramic design criteria

<End Item> structure shall be design requirements for window, glass, and ceramic shall be in accordance with SSP 30560, section 3.0 requirements.

3.2.10.11 Pressure systems and pressure vessels

Pressure vessels shall be designed in accordance with SSP 30559, Pressurized Storage Containers, and MIL-STD-1522 as modified by SSP 30558, Pressure Vessels.

3.2.10.12 Bolts

Bolt design in preloaded joints shall be in accordance with NSTS 08307, Criteria for Preloaded Bolts. Alternatives shall require NASA approval prior to implementation.

3.2.10.13 Materials selection

<End Item> structrual material selection shall be in accordance with SSP 30233.

3.2.10.14 Nonstandard fasteners

Use of nonstandard fasteners in the <End Item> structural design shall be in accordance with SSP 30559, section 3.8, Non standard Fasteners.

3.2.10.15 Fail-Safe or Safe-Life

Flight element primary structure shall be designed fail-safe or have safe-life, or be a low-risk fracture part as defined in SSP 30558, Fail Safe Part, and, Safe Life Verification.

3.2.10.16 Thermal Effects

<End Item> structure shall meet performance requirements specified herein when applicable thermal effects as described in 3.2.5.1 (of S683-29523D, Prime Item Development Specification for the U.S. Laboratory Module) are combined with induced static and dynamic loads, including thermally induced structural interface loads defined in Table XXXIV. Static loads at USL structural interfaces are defined in 3.3.12.1.7 of S683-29523D, Prime Item Development Specification for the U.S. Laboratory Module.

TABLE XXXIV. Thermally induced structural interface loads			
Event	Document	Paragraph	Description
Orbiter Flight	SD77-SH-0214	Quasi-static Models and Deflection Data Management/Control System	Orbiter bay wall deflections due to Ascent, On-Orbit, and Ascent thermal effects
On-orbit	SSP 42097	Structural Loads	Thermally - induced structural loads
On-Orbit	SSP 41141	Structural Loads	Thermally - induced/structural loads
On-Orbit	SSP 42011	Thermal Loads	Thermally - induced ITS S0 to USL interface loads
On-Orbit	SSP 41143	Structural Loads	Thermally - induced structural loads

3.2.10.17 Shuttle Payload Configuration Design Loads

For lift-off, ascent, on orbit, descent, landing, and emergency landing using Shuttle, International Space Station structure shall be designed to maintain required functionality and positive margins when subjected to all static and dynamic loads and thermal environments as defined in NSTS 07700, Volume XIV, Space Shuttle System Payload Accommodations, and ICD 2-19001, Shuttle Orbiter/Cargo Standard Interfaces.

3.2.10.17.1 Re-distributed Loads

Structure whose load paths are controlled by electro-mechanical devices shall be designed to maintain the factors of safety of section 3.3 on the redistributed loads after 1 or 2 credible electro-mechanical system failures. Operational procedures may be used to restore the load path or limit the applied loads after the first failure in order to maintain the requried factors of safety.

3.2.10.17.2 Factors of Safety - Test verified structure

All International Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified per SSP 30599, Rev.B. (See 30599, Table 3.3.1-1)

3.2.10.17.3. Shuttle Transport To/From Orbit

For Space Shuttle payloads, verification of primary payload structure for strength integrity by analysis only is not considered to be a viable option without prior and written approval of the Space Shuttle/Payloads Structural/Mechanical Working Group.

3.2.10.17.4 Emergency Landing

The structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in the ICDs between the Orbiter and the payload. Structural verification for these loads may be certified by analysis only.

3.3 SSP 30559 AND SSP 30558 REQUIREMENTS

3.3.1 SSP 30559, Structural Design and Verification Requirements:

3.1.3 Strength and Stiffness

International Space Station structure shall have adequate strength and stiffness in all necessary configurations and stages, to support ultimate load without failure. Detrimental deformation shall not occur at limit loads imposed during Shuttle transportation and on-orbit operations, or during proof or acceptance testing. All flight primary structure shall be designed to be either fail-safe, have safe-life, or be a low risk fracture part as defined in SSP 30558, Fracture Control Requirements for International Space Station.

3.1.9 Design Requirements for Pressure System

3.1.9.1 Fracture Control

Pressure vessels shall be designed and fabricated under an approved fracture control program and be in accordance with requirements specified in SSP 30558, Fracture Control Requirements for International Space Station, Section 4.4.

3.1.9.2 Pressure Control

Where pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) are used to control pressure, they shall collectively be two-fault tolerant from causing the pressure to exceed the MDP of the system.

3.1.9.3 Dewars

Dewar/cryostat systems shall be designed in accordance with the pressure vessel requirements in SSP 30558, section 4.4. and the following:

(a) Pressure containers shall be leak-before-bust (LBB) designs were possible as determined by fracture mechanics analysis. Containers of hazardous fluids and all non-LBB designs must employ a fracture mechanics safe-life approach to assure safety of operation.

(b) MDP assessment for the pressure container shall envelop the pressure achieved under maximum venting conditions.

(c) Outer shells (i.e., vacuum jackets) shall have pressure relief capability to preclude rupture in the event of pressure container leakage. If pressure containers do not vent external to the dewar but instead vent into the volume contained by the outer shell, the outer shell relief devices shall be capable of venting at a rate to release full flow without outer shell rupture. Relief devices shall be redundant and individually capable of full flow.

(d) Pressure relief devices which limit maximum design pressure shall be certified to operate at the required conditions of use. Certification shall include testing of the same part number from the flight lot under the expected use conditions.

(e) Nonhazardous fluids may be vented into the cargo bay if analysis shows that a worst case credible volume release will not affect the structural integrity or thermal capability of the Orbiter.

(f) The reproof test factor for each flight pressure container shall be a minimum of 1.1 times MDP. Qualification bust and pressure cycle testing is not required if all the requirements of paragraphs 3.1.9 are met. The structural integrity for external load environments shall be demonstrated in accordance with NSTS 14046.

3.1.9.4 Secondary Volumes

Secondary compartments or volumes that are integral or attached by design to pressure system components and which can become pressurized as a result of a credible single barrier failure shall be designed for safety consistent with structural requirements. Redundant seals in series which have been acceptance pressure tested individually prior to flight shall not be considered credible single barrier failure. Failures of structural parts such as pressure lines and tanks, and properly designed and tested welded or brazed joints shall not be considered single barrier failures. In order to be classified as non-credible failure, the item shall be designed for a safety factor of 2.5 on the MDP, and shall be certified for all operating environments including fatigue conditions. If extenal leakage would not present a catastrophic hazard, the secondary volume shall either be vented or equipped with a relief provision in lieu of designing for system pressure.

3.1.9.5 Flow Induced Vibration

All flexible hoses and bellows shall be designed to exclude or minimize flow induced vibrations in accordance with MSFC-DWG-20M02540. Certification of hardware shall be in accordance with NSTS 08123. When certification by test is required, requirements in MSFC-SPEC-626 shall apply.

3.1.9.6 Pressure Stabilized Vessels

Pressure vessels which are pressure-stabilized and must contain a minimum pressure to maintain the required ultimate factors of safety to insure structural integrity under launch and landing loads shall meet the following requirements:

a) The existence of the minimum required pressure shall be verified prior to the application of safety critical loads into the system. This verification shall include a single fault tolerant pressure decay monitoring technique which is implemented such that the system pressure decay characteristics can be certified to insure minimum design safety factors will exist at the time of subsequent structural load application.

3.1.9.7 Burst Discs

When burst discs are used as the second and final control of pressure to meet the requirements of 3.1.9.2, they shall be designed to the following requirements:

a) Burst discs shall incorporate a reversing membrane against a cutting edge to insure rupture.

b) Burst disc design shall not employ sliding parts or surfaces subject to friction and/or galling.

c) Stress corrosion resistant materials shall be used for all parts under continuous load.

d) The burst disc design shall be qualified for the intended application by testing at the intended use conditions including temperature and flow rate.

e) Qualification shall be for the specific part number used, and it shall be verified that no design or material changes exist between flight assemblies and assemblies making up the qualification database.

f) Each flight assembly shall be verified for membrane actuation pressure either by, (1) use of special tooling or procedures to prevent cutting-edge contact during the test or, (2) demonstration of a rigorous lot screening program approved by the Shuttle Payload Safety Review Panel.

3.1.9.8 Mechanical properties

Mechanical properties of structural materials shall be in accordance with MIL-HDBK-5, MIL-HNBK-17, or other sources in accordance with SSP 30559, section 3.6.2, Structural Material Allowable Properties.

3.3.2 SSP 30558, Fracture Control Requirements for International Space Station:

4.4.1 Pressure Vessels

4.4.1.1

Pressure vessels, as defined in Appendix B of SSP 30558, shall comply with requirements in Sections 4 and 5 of MIL-STD-1522A, Standard General Requirements for Safe Design and Operations of Pressurized Middile and Space Systems, including revisions as of November 1986, modified as follows:

(a) In the event of conflict in requirements between MIL-STD-1522A and this document, the requirements of this document shall take precedence.

(b) Approach "B" of Figure 2 in MIL-STD-1522A is not acceptable and shall not be used.

(c) Pressure vessels whose failure at Maximum Design Pressure (MDP) would not be leak before burst, or would release a hazardous fluid, or whose loss of pressure would be potentially catastrophic, shall be safe-life vessels. All other pressure vessels shall be either safe-life or leak before burst at MDP.

(d) MDP as defined in Appendix B, shall be substituted for all reference to maximum expected operating pressure in MIL-STD-1522A.

(e) For metal lined pressure vessels having an overwrapped composite structure, the fracture control for safe life and failure mode shall be applied to the liner. The overwrap shall in addition satisfy paragraph 4.7.4 of this document.

(f) In addition to other required analyses, composite pressure vessels shall be assessed for adequate stress rupture life and effects of atomic oxygen.

(g) NDE of safe life pressure vessels shall include inspection of welds before and after proof testing.

(h) Controls shall be implemented to ensure compatibility of vessel material with fluid used in cleaning, test and operation.

(i) An acceptable approach to LBB is to show that a through the thickness crack of length ten times the wall thickness is stable (i.e., $K_{max} < K_c$) at MDP. If fracture mechanics data are not available, or reliable conservative estimates of properties cannot be made, a vessel test shall be conduced to verify leak-before-burst capability.

(j) For low cycle applications a proof test of each flight pressure vessel to a minimum of 1.5 times MDP and a fatigue analysis showing the greater of 500 pressure cycles or 10 lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of SSP 30559 and MIL-STD-1522A, Approach A.

4.4.2 Pressure System Components

4.4.2.1

Pressure system components (or equipment) not meeting the definition of pressure vessels given in Appendix B of SSP 30558, shall be considered fracture critical if they contain hazardous fluids or if loss of pressurization would result in a catastrophic hazard. All fusion weld joints on Fracture Critical components shall be inspected using a qualified NDE method. In instances where NDE is not feasible, or is incapable of being dealt with successfully, the manufacturer will employ a verification by sampling procedure for establishing the quality of uninspectable welds. This option requires NASA or International Partner approval. Cracks or any other type of flaw indication not meeting specification requirements shall be cause for rejection of these components. Safe-life analysis is not required for fracture critical pressurized lines, fittings and components which are proof tested to the factor of safety requirements of SSP 30559, Structural Design and Verification Requirements, section 3.3. In addition to proof testing of parts during individual acceptance, pressure integrity shall be verified at the system level.

5.0 OPERATIONAL SAFETY REQUIREMENTS

5.1 EVA Activity Safety

All ISS requirements for EVA shall be defined and documented in the MIP Operations Approval (from Space Shuttle Astronaut AIT, EVA System AIT, and Space Shuttle Missions AIT) and shall be required for any EVA task. (Ref. COU SSP 50011-01 Rev. B; Para. 4.2.2; Oct. 19, 1994)

5.1.3.1 For Shuttle Loads

The International Space Station structural design and verification requirements for the transport phases to and from orbit shall be consistent with the requirements for Shuttle payloads specified in NSTS 14046. ISS elements shall be verified by test and/or analysis to the ascent vibro-acoustic environment defined in ICD 2-19001.

5.1.3.6 Verification Of Beryllium Structures

Verification of Beryllium structures shall be in accordance with NSTS's 14046, section 5.1.1.1.

Appendix A - Acronym Listing

AC	Alternating Current
BFO	Blood Forming Organs
CETA	Crew and Equipment Translation Aids
CO2	Carbon Dioxide
dB	Decibel
DC	Direct Current
EVA	Extravehicular Activity
ISS	International Space Station
IVA	Intravehicular Activity
IMV	Intermodule Venitlation (System)
MDP	Maximum Design Pressure
MEQ	Milliequilivants
MPE	Maximum Permissible Exposure
MT	Mobile Transporter
NSI	NASA Standard Initiator
NSTS	National Space Transportation System
ORU	Orbital Replacement Unit
OSE	Orbital Support Equipment
PBA	Portable Breathing Apparatus
PFE	Portable Fire Extinguisher
PIP	Payload Integration Plan
RMS	Remote Manipulator Subsystem
RTM	Real-Time Monitor
SMAC	Spacecraft Maximum Allowable Concentration
STS	Space Transportation System

APPENDIX B - GLOSSARY OF TERMS

DEFINITIONS

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or major ground facility. For safety failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to elements fo the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezuous and dockinng operations with ISSSA launch elements.

Credible failure - A condition that has a potential of occurring based on actual failure modes in similar systems.

Critical Hazard - Any condition which may cause a nondisabling personnel injury, severe occupational illness; loss of a~~n~~ major ISS element, on-orbit life sustaining function or emergency system, or involves damage to: Orbiter or a ground facility. For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the ciritical path for station survival or which can be restored through contingency repair.

Design for Minimum Risk - Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance. criteria. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance must be imposed upon external system that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure of the pressure vessel. Examples are mechanisms, structures, glass, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Hazard - The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Hazard Controls - Design or operational features used to reduce the likelihood of occurrence of a hazardous effect. Hazard controls are implemented in the following order of precedence:

a. Elimination of hazard through removal of hazardous sources and operations.

b. Ensure inherent safety through provisions of appropriate design features, materials and parts selection, and safety factors. Design considerations to include damage control, containment, isolation of potential hazards and failure tolerance considerations.

c. Reduce hazard to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

d. Minimize the effects of potential hazards through the use of warning devices, crew operational procedures or protective clothing and/or equipment.

Hazardous command - A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard.

Independent inhibit - Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

Independent Safing Action - A safing action is an action generated by a nonfailed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent both safing actions from transitioning the system to a safe state.

Inhibit - a. Hardware implementation: A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.). b. Software implementation: A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available. Note: Software inhibits are not counted in meeting safety requirements for multiple inhibits.

Interlock - A design feature that ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed.

Local control - A capability to accomplish a function at the directin of the crew within the applicable on-orbit moudule and also prevent reconfiguration of the function by an external entity during the specified period.

M/OD Critical Item - An item is deemed to be M/OD critical when effects resulting from meteoroid or orbital debris impact will endanger the crew or Space Statioin survivability.

Near Real Time Monitoring - Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). The capability of the hardware and software to provide the updated data for near real-time monitoring data is gennerally the lowest abailale frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Operator error - An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

Rapid Safing - The capability of the orbiter to accomplish an emergency deorbit or a deobit contingency to the next primary landing site.

Radiation, Ionizing - TBD

Real Time Monitoring - Notification of changes in inhibit or safety status to the crew at a rate adequate to allow for appropriate reaction to a change in the status. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user t react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

Safe - A general term denoting an acceptable level of risk, relative freedom from and low probability of: personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

Safety critical - A condition, event, operation, process, function, equipment or system (including software and firmware) with potential for personnel injury or loss, or with potential for loss or damage to vehicles, equipment or facilities, loss or excessive degradation of the function of critical equipment, or which is necessary to control a hazard.

Safety critical software - Software which:

a. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly, could result in control function loss or error which could cause a hazard

b. Monitors the condition or state of hardware components and, if monitoring is not performed or is performed incorrectly, could provide data which results in erroneous operator or companion system decisions which could cause a hazard

c. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly in conjunction with human error or hardware failure, could cause a hazard.

Safing - Event or sequence of events necessary to place systems, subsystems or component parts into predetermined safe conditions.

Appendix C - Traceability of NSTS 1700.7B to SSP 50021

NSTS 1700.7B Paragraph number	NSTS 1700.7B	
100	PURPOSE This document establishes the safety policy and requirements applicable to Space Transportation System (STS.) payloads and their ground support equipment (GSE.).	**SSP 50021 Section 1.1 Purpose** The purpose of SSP 50021 is to provide a single repository for the ISS and Shuttle jointlyagreed upon safety requirements to be imposed on the ISS program. This allows the Safety Review Panel to assess flight hardware compliance to the program safety requirements.
101	SCOPE These requirements are intended to protect flight and ground personnel, the STS, other payloads GSE, the general public, public-private property, and the environment from payload-related hazards. This document contains technical and system safety requirements applicable to STS payloads (including payload-provided ground and flight support systems) during ground and flight operations.	**SSP 50021 Section 1.2 Scope** This document provides the requirements which are intended to protect flight and ground personnel, the ISS, the STS, payloads, GSE, the general public, public-private property, and the environment from ISS-related hazards. This document contains technical requirements applicable to ISS LPs during ground processing, launch, on-orbit flight operations, and return. The requirements contained herein apply to ISS (USOS, NASA, RSA, ESA, NASDA, ISA, CSA) flight systems and flight support equipment at assembly complete only.
101.1	GSE Design and Ground Operations For additional safety requirements which are unique to ground operations and GSE design, one shall refer to the joint Space and Missile Test Organization (SAMTO)/Kennedy Space Center (KSC), Handbook, SAMTO HB S-100/KHB 1700.7.	**SSP 50021 Section 1.2 Scope** These requirements do not apply to the design, development, or operation of ground support equipment. For ground support equipment requirements, refer to the joint Space and Missle Test Organization (SAMTO)/Kennedy Space Center(KSC) Handbook, SAMTO HB S-100/KHB 1700.7, and SSP 50004 Ground Support Equipment Design Requirements.

101.2	Flight Rules Flight rules will be prepared for each STS mission that outline pre-planned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. These flight rules are not additional safety requirements, but do define actions for completion of the STS flight consistent with crew safety. Compliance with minimum safety requirements of this document will not insure the mission success of a payload. For example, if an STS user only monitors two of three inhibits to a catastrophic hazardous function (this is the minimum requirement specified in paragraph 201.3), a flight rule related to the loss of a monitored inhibit may be imposed which is not favorable to the mission success of the payload.	**SSP 50021 Section 1.2.2 Mission Rules** Mission Rules will be prepared for each ISS mission that outline preplanned decisions designed to minimize the amount of real-time rationalization required when anomalous situations occur. These mission rules are not additional safety requirements, but do define actions for completion of the ISS consistent with crew safety. Compliance with minimum safety requirements of this document will not insure the mission success of an ISS operation.
102	**RESPONSIBILITY**	
102.1	Payload Organization It is the responsibility of each payload organization to assure the safety of its payload and to implement the requirements of this document. Where a payload integration of mission management organization is identified, that organization interfaces with the NSTS on behalf of the group of individual payload elements or experiments under its control. That organization has the responsibility to assure that the individual payload elements are safe and meet the requirements of this document. That organization also has the responsibility to assure that interaction among its payload elements doe snot create a hazard.	**SSP 50021 Section 1.4.1 ISS** It is the responsibility of each ISS program Participants (NASA, RSA, ESA, NASDA, ISA, CSA) to assure the safety of ISS systems and identify any non-compliances with the applicable specification requirements or the requirements herein. The ISS Safety and Mission Assurance Office within the ISS Program Office is responsible for assuring the requirements herein are properly and completely included and allocated in the ISS specifications and requirement documents. The ISS prime contractor will show traceability of the requirements herein to the coresponding requirement(s) in the ISS specifications and will evaluate compliance to this document. The [insert SRP or OE here] is responsible for maintenance and configuration control of this document.

102.2	NSTS It is the responsibility of the NSTS to interface with the responsible payload organization to review the payload for adequate safety implementation. It is also the responsibility of the NSTS to assure that interaction among mixed payloads, and between payloads and the STS, does not create a hazard.	**SSP 50021 Section 1.4.1 ISS** It is the responsibility of each ISS program Participants (NASA, RSA, ESA, NASDA, ISA, CSA) to assure the safety of ISS systems and identify any non-compliances with the applicable specification requirements or the requirements herein. The ISS Safety and Mission Assurance Office within the ISS Program Office is responsible for assuring the requirements herein are properly and completely included and allocated in the ISS specifications and requirement documents. The ISS prime contractor will show traceability of the requirements herein to the coresponding requirement(s) in the ISS specifications and will evaluate compliance to this document. The [insert SRP or OE here] is responsible for maintenance and configuration control of this document.
103	IMPLEMENTATION This document identifies the safety policy and requirements which are to be implemented by the payload organization. The implementation of safety requirements by the payload organization will be assessed by the NSTS during the safety review process and must be consistent with hazard potential. The NSTS assessment of safety compliance will include a complete review of the safety assessment reports (paragraph 301) and may include audits and safety inspections of the flight hardware. The detailed interpretations of these safety requirements will be by the NSTS, and will be determined on a case-by-case basis consistent with the payload's hazard potential. The following supplementary documents have been issued to assist payload organization in complying with the requirements of this document.	**SSP 50021 Section 1.4.1 ISS** It is the responsibility of each ISS program Participants (NASA, RSA, ESA, NASDA, ISA, CSA) to assure the safety of ISS systems and identify any non-compliances with the applicable specification requirements or the requirements herein. The ISS Safety and Mission Assurance Office within the ISS Program Office is responsible for assuring the requirements herein are properly and completely included and allocated in the ISS specifications and requirement documents. The ISS prime contractor will show traceability of the requirements herein to the coresponding requirement(s) in the ISS specifications and will evaluate compliance to this document. The [insert SRP or OE here] is responsible for maintenance and configuration control of this document.

103.1	Implementation Procedure NSTS 13830, a jointly issued Johnson Space Center (JSC.) and Kennedy Space Center (KSC) document, has been published to assist the payload organization in implementing the system safety requirements and to define further the safety analyses, data submittals, and safety assessment review meetings. NSTS 13830 identifies the respective roles of the NSTS flight operator and the NSTS launch/landing site operator. It reflects a basic policy of commonality, compatibility, and coordination between the NSTS flight and ground elements in the implementation effort.	**SSP 30599**, Space Station Safety Review Process Section 1.1 Purpose The purpose of SSP 30599 is to define the safety review process for ISS elements (flight and ground), support equipment, and integration of experiment racks into modules. The safety review process for ISS payload experiments (flight and ground) including integration of experiments into the racks is defined in National Space Transportation System (NSTS) 13830, Implementation Procedure for NSTS Payloads System Safety Requirements.
103.2	Interpretations of Requirements NSTS 18798 is a collection of interpretations of requirements relative to specific payload designs. These interpretations shall be applied to payloads that utilize similar design solutions. Addenda to NSTS 18798 are distributed to payload organizations as additional interpretations are generated.	**See attached matrix for Interpretation Letters**
104	GLOSSARY OF TERMS For definitions applicable to this document, see Appendix A.	**SSP 50021, Appendix B**
105	APPLICABLE DOCUMENTS A list of documents which are referenced in this document is in Appendix B.	**SSP 50021, Section 2.0, Applicable Documents**
106	FIGURES Figures referred to in the text are contained in Appendix C.	**N/A**

200	GENERAL The following requirements are applicable to all payloads. When a requirement cannot be met, a noncompliance report must be submitted in accordance with NSTS 13830 for resolution.	**SSP 50021, 1.5 Waivers And Deviations** Request for waiver or deviation shall be made to the ISS Program Office, in accordance with Configuration Management Requirements. **SSP 30599, 1.2 Scope** Any request for waiver or deviation from the requirements of this document shall be made to the ISS in accordance with Configuration Management Requirements.
200.1	Design to Tolerate Failures Failure tolerance is the basic safety requirement that shall be used to control most payload hazards. The payload must tolerate a minimum number of credible failures and/or operator errors determined by the hazard level. This criterion applies when the loss of a function or the inadvertent occurrence of a function results in a hazardous event.	**Definition**
200.1a	Critical Hazards Critical hazards shall be controlled such that no single failure or operator error can result in damage to STS equipment, a non-disabling personnel injury, or the use of unscheduled safing procedures that affect operations of the Orbiter or another payload.	**SSP 50021** **Section 3.3.6.1.2 Critical Hazards.** The <End Item> shall be designed such that no single failure or single operator error can result in a nondisabling personnel injury, severe occupational illness; loss of an ISS on-orbit life sustaining function or emergency system, or involves damage to one of the following: Orbiter or a ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.
200.1b	Catastrophic Hazards. Catastrophic hazards shall be controlled such that no combination of two failures or operator errors can resulting the potential for a disabling or fatal personnel injury or loss of the Orbiter, ground facilities or STS equipment.	**SSP 50021** **Section 3.3.6.1.1 Catastrophic Hazards** The <End Item> shall be designed such that no combination of two failures, or two operator errors (See 6.1), or one of each can result in a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or major ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

200.2	Design for Minimum Risk Payload hazards which are controlled by compliance with specific requirements of this document other than failure tolerance are called "Design for Minimum Risk" areas of design. Examples are structures, pressure vessels, pressurized line land fittings, functional pyrotechnic devices, mechanisms in critical applications, material compatibility, flammability, etc. Hazard controls related to those areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the payload organization and the NSTS. Minimum supporting data requirements for these areas of design have been identified in NSTS 13830.	**SSP 50021** **Section 3.3.6.1.3 Design for minimum risk.** Hazards related to "Design for Minimum Risk" areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of "Design for Minimum Risk" areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.
200.3	Environmental Compatibility A payload shall be certified safe in the applicable worst case natural and induced environments defined in the payload integration plan (PIP.) and/or interface control document (ICD.).	**SSP 50021** **Section 3.3.6.1.8 Environmental compatibility.** <End Item> functions shall be safe in the applicable worst case natural and induced environments defined in paragraph 3.2.5 (2.6 for IPs) , "Environmental Conditions" or as defined in a payload integration plan , mission integration plan and/or interface control document. **Section 3.2.5.4 Environmental Conditions** The <End Item> shall satisfy the requirements of this specification when subjected to the environmental conditions for the environments and environmental phases specified below.
200.4	STS Services	**Title**
200.4a	Safe Without Services. Payloads shall be designed to maintain fault tolerance or safety margins consistent with the hazard potential without ground or flight NSTS services. During Orbiter emergency conditions, power will be provided temporarily to payloads for payload safing and verification if necessary. Subsequent to payload safing, power may not be available to payloads. Monitoring is not mandatory under these conditions.	**SSP 50021** **Section 3.3.6.13.1 Safe Without Space Shuttle Program Services.** **Section 3.3.6.13.1.1 Fault tolerance/safety margins** The <End Item> shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services. **Section 3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions** During Orbiter emergency conditions, <END ITEM> shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

200.4b	Critical Orbiter Services. When NSTS services are to be utilized to control payload hazards, the integrated system must meet the failure tolerance requirements of paragraph 200.1 and adequate redundancy of the NSTS services must be negotiated. JSC 16979 specifies the fault tolerance of Orbiter-provided payload services which must be used when conducting payload hazard analyses. The payload organization must provide a summary of the hazards being controlled by STS services in the safety assessment report (see paragraph 301) and document in the individual hazard reports those Orbiter interfaces used to control and/or monitor the hazards. Those payload hazards being controlled by Orbiter-provided services will require post-mate interface test verification for both controls and monitors. In addition, the payload organization shall identify in the payload/Orbiter ICD those Orbiter interfaces used to control and/or monitor the hazards.	**SSP 50021** **Section 3.3.6.13.2 Critical Orbiter Services.** When Orbiter services are to be utilized to control <End Item> hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.
201	CONTROL OF HAZARDOUS FUNCTIONS	**Title**
201.1	General Hazardous functions are operational events (e.g., motor firings, appendage deployments, stage separations, and active thermal control) whose inadvertent operations or loss may result in a hazard.	**Definition**
201.1a	Inhibits. An inhibit is a design feature that provides a physical interruption between an energy source and a function (a relay or transistor between a battery and a pyrotechnic initiator, a latch valve in the plumbing line between a propellant tank and a thruster, etc.). Two or more inhibits are independent if no single credible failure, event, or environment can eliminate more than one inhibit.	**Definition**
201.1b	Controls. A device or function that operates an inhibit is referred to as a control for an inhibit. Controls do not satisfy the inhibit or failure tolerance requirements for hazardous functions. The ”electrical inhibits” in a liquid propellant propulsion system ([paragraph 202.2a(3)]) are exceptions in that these devices operate the flow control devices (i.e., referred to as inhibits and not as controls.	**Definition**

201.1c	Monitors. Monitors are used to ascertain the safe status of payload functions, devices, inhibits and parameters. Monitoring circuits should be designed such that the information obtained is as directly related to the status of the monitored device as possible. Monitor circuits shall be current limited or otherwise designed to prevent operation of the hazardous functions with credible failures. In addition, loss of input or failure of the monitor should cause a change in state of the indicator. Monitoring shall be available to the launch site when necessary to assure safe ground operations. Notification of changes in the status of safety monitoring shall be given to the flight crew in either near-real-time or real-time.	**SSP 50021** **Section 3.3.6.2.2 Monitors.** **Section 3.3.6.2.2.1 Status information** Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device. **Section 3.3.6.2.2.2 Hazardous function operation prevention** Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function. **Section 3.3.6.2.2.3 Loss of input or failure** Loss of input or failure of the monitor shall be identifiable. **3.3.6.2.2.4 Launch site availability** Monitoring shall be available to the launch site when necessary to assure safe ground operations. **3.3.6.2.2.5 Flight crew availability** Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.
201.1c(1)	Near-Real-Time Monitoring. Near-real-time monitoring (NRTM.) is defined as notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). NRTM may be accomplished via ground crew monitored telemetry data. Switch talk backs shall not be used as the only source of safety monitoring when the hazard exists during crew sleep periods.	**SSP 50021** **Section 3.3.6.2.3 Near-real time monitoring.** Near-real time monitoring of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, "Respond to Loss of Function". The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard.

201.1c(2)	Real-Time Monitoring. Real-time monitoring (RTM) is defined as immediate notification to the crew. RTM shall be accomplished via the use of the Orbiter failure detection and annunciation system or by ground crew monitored telemetry data. An exception to this could be where RTM is necessary only during payload operations. Under these conditions, switch panel talk back monitoring is acceptable. Real-time monitoring of inhibits to a catastrophic hazardous function is required when changing the configuration of the applicable payload system or when the provisions of paragraph 204 are implemented for flight crew control of the hazard. If ground monitoring is used to meet real-time monitoring, a continuous real-time data link (containing the applicable safety parameters) must be assured by the payload and continuous communications between the flight and ground crews must be established and maintained during the required period.	**SSP 50021** **Section 3.3.6.2.4 Real Time Monitoring.** **Section 3.3.6.2.4.1 Maintain status of hazard controls** The <End Item> shall provide real-time monitoring (See 6.1) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the <End Item> is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors. **Section 3.3.6.2.4.2 Crew response time and safing procedures** If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required. **Section 3.3.6.2.4.3 Ground monitoring** If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within time to effect of the hazard upon loss of communications with the ground.
201.1c(3)	Unpowered Bus Exception. Monitoring and safing of inhibits for a catastrophic hazardous function will not be required if the function power is de-energized (i.e., an additional fourth inhibit is in place between the power source and the three required inhibits) and the control circuits for the three required inhibits are disabled (i.e., no single failure in the control circuitry will result in the removal of an inhibit) until the hazard potential no longer exists.	**SSP 50005**
201.1d	Use of Timers. When timers are used on deployable payloads to control inhibits to hazardous functions, complete separation of the payload from the Orbiter may be achieve prior to the initiation of the timer. If credible failure modes exist that could allow the timer to start prior to a complete separation, a safing capability must be provide.d If this safing is via a radio frequency (RF) command, then the command capability must be provided to the flight crew.	**SSP 50005**
201.1e	Computer-Based Control Systems	**SSP 50038 Computer Based Control System Safety Requirements**

201.1e(1)	Active Processing to Prevent a Catastrophic Hazard. While a computer system is being used to actively process data to operate a payload system with catastrophic potential, the catastrophic hazard must be prevented in a two-failure tolerant manner. One of the methods to control the hazard must be independent of the computer system. A computer system shall be considered zero fault tolerant in controlling a hazardous system (i.e., a single failure will cause loss of control), unless the system utilizes independent computers, each executing uniquely developed instruction sequences to provide the remaining two hazard controls.	**SSP 50038 Computer Based Control System Safety Requirements**
201.1e(2)	Control of Inhibits. The inhibits to a hazardous function may be controlled by a computer-based system used as a timer, provided the system meets all the requirements for independent inhibits.	
201.2	Functions Resulting in Critical Hazards A function whose inadvertent operation could result in a critical hazard must be controlled by two independent inhibits, whenever the hazard potential exists. Requirements for monitoring (paragraph 201.1c) of these inhibits and for the capability to restore inhibits to a safe condition are normally not imposed, but may be imposed on a case-by-case basis. Where loss of a function could result in a critical hazard, no single credible failure shall cause loss of that function.	**SSP 50021** **Section 3.3.6.1.4 Control of functions resulting in critical hazards.** **Section 3.3.6.1.4.1 Inadvertent operation resulting in critical hazards.** A function whose inadvertent operation could result in a critical hazard shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels. **Section 3.3.6.1.4.2 Loss of function resulting in critical hazards.** Where loss of a function could result in a critical hazard, no single credible failure shall cause loss of that function and the function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and Respond to Loss of Function". Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

201.3	Functions Resulting in Catastrophic Hazards A function whose inadvertent operation could result in a catastrophic hazard must be controlled by a minimum of three independent inhibits, whenever the hazard potential exists. One of these inhibits must preclude operation by an RF command or the RF link must be encrypted. In addition, the ground return for the function circuit must be interrupted by one of the independent inhibits. At least two of the three required inhibits shall be monitored (paragraph 201.1c). If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.	**SSP 50021** **Section 3.3.6.1.5 Control of functions resulting in catastrophic hazards.** **Section 3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards** Compliance with requirements of this paragraph may be accomplished at the end Item level or through a combination of hazard controls at the Segment/System levels. **Section 3.3.6.1.5.2 Loss of function resulting in catastrophic hazards** Compliance with requirements of this paragraph may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels. a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function. b. The function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function".
202	SPECIFIC CATASTROPHIC HAZARDOUS FUNCTIONS In the following subparagraphs, specific requirements related to inhibits, monitoring, and operations are defined for several identified potentially catastrophic hazardous functions.	**Title**
202.1	Solid Propellant Rocket Motors Premature firing of a solid propellant rocket motor, while the payload is closer to the Orbiter than the minimum safe distance, is a catastrophic hazard.	**N/A No Solid Rocket Motors identified on ISS**
202.1a	Safe Distance. The safe distance for firing a solid rocket motor is defined as the separation distance achieved 45 minutes after deployment with the payload coasting with a minimum separation velocity of 1 foot per second. Payloads with a positive separation velocity less than 1 foot per second either:	**N/A; No Solid Rocket Motors identified on ISS**
202.1a(1)	Shall provide an RF command capability as a flight crew function to inhibit automatic sequencing until a safe distance is assured; or	**N/A; No Solid Rocket Motors identified on ISS**

202.1a(2)	Shall initiate payload sequencing (such as, starting a timer that will remove inhibits to cause engine firing) by a real-time RF command with prior NSTS coordination and approval and the RGF command to start sequencing shall not be sent until a safe separation distance is assured. For payloads deployed with the Remote Manipulator System (RMS), sequencing shall be initiated by a real time RF command.	**N/A; No Solid Rocket Motors identified on ISS**
202.1b	Safe and Arm (S&A) Device. All solid propellant rocket motors shall be equipped with an S&A device that provides a mechanical interrupt in the pyrotechnic train immediately downstream of the initiator. The S&A device shall be designed and tested in accordance with provisions of MIL-STD-1576. If the S&A device is to be rotated to the arm position prior to the payload achieving a safe distance from the Orbiter: rotation must be a flight crew function and must be done as part of the final deployment activities of the payload; and the initiator must meet the requirements of paragraph 210. The S&A must be in the safe position during Orbiter boost and entry. There must be a capability to resafe the S&A device: if the S&A device is to be rotated to the arm position while the payload is attached to the Orbiter; or if the solid rocket motor propulsion subsystem does not qualify for the unpowered bus exception of paragraph 201.1c(3). In determining compliance with paragraph 201.1c(3), the S&A device in the ”safe” position shall be counted as one of the required inhibits.	**N/A; No Solid Rocket Motors identified on ISS**
202.1c	Electrical Inhibits. In addition to the S&A, there shall be at least two independent electrical inhibits, to prevent firing of the motor if the S&A device will be in the ”safe” position until the payload reaches a safe distance from the Orbiter. There shall be at least three independent electrical inhibits, in addition o the S&A, if the S&A device will be rotated to the arm position prior to the payload reaching a safe distance from the Orbiter.	**N/A; No Solid Rocket Motors identified on ISS**
202.1d	Monitoring. Monitoring requirements are a function of the design and operations as follows:	**N/A; No Solid Rocket Motors identified on ISS**

202.1d(1)	No Rotation of the S&A Prior to a Safe Distance. The capability to monitor the status of the S&A device and one electrical inhibit in near real-time is required until final separation of the payload from the Orbiter. No monitoring is required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3).	**N/A; No Solid Rocket Motors identified on ISS**
202.1d(2)	S&A Will be Rotated to Arm Prior to a Safe Distance. Prior to rotation of the S&A and separation of the payload from the Orbiter, the flight or ground crew must have continuous real-time monitoring to determine the status of the S&A and to assure that two of the three electrical inhibits are in place (paragraph 201.1c(2).	**N/A; No Solid Rocket Motors identified on ISS**
202.2	Liquid Propellant Propulsion Systems	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2a	Premature Firing. The premature firing of a liquid propellant propulsion system before the payload reaches a safe distance from the Orbiter is a catastrophic hazard. Each propellant delivery system must contain a minimum of three mechanically independent flow control devices in series to prevent engine firing. A bipropellant system shall contain a minimum of three mechanically independent flow control devices in series both in the oxidizer and fuel sides of the delivery system. These devices must prevent contact between the fuel and oxidizer as well as prevent expulsion through the thrust chamber(s). Except during ground servicing and as define din paragraph 202.2a(2)(a), these devices will remain closed during all ground and flight phases until the payload reaches a safe distance from the Orbiter. A minimum of one of the three devices will be fail-safe, i.e., return to the closed condition in the absence of an opening signal.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**

202.2a(1)	Safe Distance Criteria. The hazard of engine firing close enough to inflict damage to the Orbiter due to heat flux, contamination, and/or perturbation of the Orbiter, is in proportion to the total thrust imparted by the payload in any axis and shall be controlled by establishing a safe distance for the event. The safe distance shall be determined using Figure 1 (see Appendix C). For large thruster systems with greater than 10 pounds total thrust, the collision hazard with the Orbiter mus be controlled by considering the safe distance criteria in Figure 1, together with the correct attitude at time of firing. For small reaction control system (RCS) thrusters with less than 10 pounds total thrust, the collision hazard must be controlled by the safe distance criteria in Figure 1 with consideration of many variables such as deployment method, appendage orientation, and control authority.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2a(2)	Isolation Valve. One of the flow control devices shall isolate the propellant tank(s) from the remainder of the distribution system.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2a(2)	(a) Opening the Isolation Valve. If a payload with a large liquid propellant thruster system also uses a small reaction control thruster system for attitude control, the isolation valve in a common distribution system may be opened after the payload has reached a safe distance for firing the reaction control thrusters provided the applicable requirements of paragraphs 202.2a(3) and 202.2a(4) have been met and two mechanical flow control devices remain to prevent thrusting of the larger system.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2a(2)	(b) Pyrotechnic Isolation Valves. If a normally closed pyrotechnically initiated valve is used, it may be considered equivalent to two propellant flow control devices if the following requirements are fulfilled: The structural design must preclude operation by vibration. The valve must use parent metal in which the inlet and the first flow barrier are a continuous unit of non-welded metal and the outlet and the last flow barrier are also a continuous unit of non-welded metal. The valve must be controlled by at least two independent electrical inhibits (three electrical inhibits will be required if paragraph 202.2b is applicable).	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**

202.2a(3)	Electrical Inhibits. While the payload is closer to the Orbiter than the minimum safe distance for engine firing, there shall be at least three independent electrical inhibits that control the opening of the flow control devices. The electrical inhibits shall be arranged such that the failure of one of the electrical inhibits will not open more than one flow control device. If the isolation valve will be opened under the conditions of paragraph 202.2a(2)(a) prior to the payload achieving a safe distance for firing a large thruster, three independent electrical inhibits must control the opening of the remaining flow control devices for the large thruster system.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2a(4)	Monitoring. At least two of the three required independent electrical inhibits shall be monitored by the flight or ground crew until final separation of the payload from the Orbiter. The position of a mechanical flow control device may be monitored in lieu of its electrical inhibit, provided the two monitors used to meet the above requirement are independent. Either near real-time or real-time monitoring will be required as defined in paragraphs 201.1c(1) and 201.1c(2). One of the monitors must be the electrical inhibit or mechanical position of the isolation valve. Monitoring will not be required if the payload qualifies for the unpowered bus exception of paragraph 201.1c(3). If the isolation valve will be opened prior to the payload achieving a safe distance from the Orbiter, all three of the electrical inhibits that will remain after the opening of the isolation valve must be verified safe during final predeployment activities by the flight or ground crew.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**

202.2b	Adiabatic/Rapid Compression Detonation. While the payload is inside the Orbiter cargo bay, the inadvertent opening of isolation valves in a hydrazine (N2H4) propellant system shall be controlled as a catastrophic hazard unless the outlet lines are completely filled with hydrazine or the system is shown to be insensitive to adiabatic or rapid compression detonation. Hydrazine systems will be considered sensitive to compression detonation unless insensitivity is verified by testing on flight hardware or on a high fidelity flight type system that is constructed and cleaned to flight specifications. Test plans must be submitted to the NSTS as part of the appropriate hazard report. If the design solution is to fly wet downstream of the isolation valve, the hazard analysis must consider other issues such as hydrazine freezing or overheating, leakage, single barrier failures, and back pressure relief.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2c	Propellant Overheating. Raising the temperature of a propellant above the fluid compatibility limit for the materials of the system is a catastrophic hazard. Components in propellant systems that are capable of heating the system (e.g., heaters, valve coils, etc.) shall be two-failure tolerant to heating the propellant above the material/fluid compatibility limits of the system. These limits shall be based on test data derived from NHB 8060.1 test methods or on data furnished by the payload supplier and approved by NSTS. Propellant temperatures less than the material/fluid compatibility limit, but greater than 200 degrees Fahrenheit must be approved by the NSTS. The use of inhibits, cutoff devices, and/or crew safing actions may be used to make the system two failure tolerant to overheating. Monitoring of inhibits (paragraphs 201.1c and 201.3) or of propellant temperature will be required.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**
202.2d	Propellant Leakage. A payload shall be two failure tolerant to prevent leakage of propellant into the Orbiter cargo bay past seals, seats, etc., if the leak has a flow patch to the storage vessel. If the leak is in an isolated segment of the distribution system, failure tolerance to prevent the leak will depend on the type and quantity of propellant that could be released. As a minimum such a leak will be one failure tolerant.	**The USOS does not have propulsion capability. Requirements for the RSA are TBD.**

202.3	Inadvertent Deployment, Separation, and Jettison Functions. Inadvertent deployment, separation or jettison of a payload, payload element or appendage is a catastrophic hazard unless it is shown otherwise. The general inhibit and monitoring requirements of paragraph 201 shall apply.	**SSP 50021** **Section 3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions** Inadvertent deployment, separation or jettison of the <End Item> or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4**,** 3.3.6.1.5 and 3.3.6.2.2 apply.
202.4	Planned Deployment/Extension Functions	**Title**
202.4a	Preventing Payload Bay Door Closure. If during planned payload operations an element of the payload or any payload airborne support equipment (ASE) violates the payload bay door envelope, the hazard of preventing door closure must be controlled by independent primary and backup methods. The combination of these methods must be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).	**SSP50021** **3.3.6.13.4 Planned Deployment/Extension Functions** **3.3.6.13.4.1 Violation of Orbiter payload door envelope** If a component of the <End Item> or any <End Item> orbital support equipment (OSE) violates the payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.
202.4b	Cannot Withstand Subsequent Loads. If during planned operations an element of a payload or is ASE is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent STS induced loads, there shall be two-failure tolerant design provisions to safe the payload. Safing may include deployment, jettison or provisions to change the configuration of the payload to eliminate the hazard.	**SSP 50021** **Section 3.3.6.1.6 Subsequent induced loads** If a component of the <End Item> is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard.

202.5	RF Energy Radiation Allowable levels of radiation from payload transmitter antenna systems are defined in the ICD, NSTS 07700, Volume XIV, Attachment 1 (ICD-2 19001). These levels define payload-to-RMS, payload-to-Orbiter, and payload-to-payload limits. Radiation from payload transmitter antenna systems will be not allowed while the payload bay doors are closed and will be permitted with the payload bay doors open only if the ICD limits are not exceeded. The requirements to prevent inadvertent radiation are as follows:	**SSP 50021** **Section 3.3.6.13.7 Allowable RF radiation levels** <End Item> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.
202.5a	Payload Bay Doors Open. With the payload bay doors opened, there shall be three independent inhibits whenever the impinging radiation would exceed the ICD limits.	**SSP 50021** **Section 3.3.6.13.7 Allowable RF radiation levels** <End Item> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.

202.5b	Payload Bay Doors Closed. With the payload bay doors closed, there shall be two independent inhibits if the impinging radiation would be below the ICD limits and three independent inhibits if the radiation would be above the limits.	**SSP 50021** **Section 3.3.6.13.7 Allowable RF radiation levels** <End Item> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.
202.5c	Monitoring. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachment 1 (ICD-2-19001) limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.	**SSP 50021** **Section 3.3.6.13.7 Allowable RF radiation levels** <End Item> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.
203	RETRIEVAL OF PAYLOADS	**Title**

203.1	Safing Deployable and/or free flying payloads that are designed to be retrieved or revisited shall have the capability of return systems which are hazardous to a safe condition (i.e., meet all the applicable requirements of this document).	**SSP 50021** **Section 3.3.6.2.2 Monitors.** **Section 3.3.6.2.2.1 Status information** Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device. **Section 3.3.6.2.2.2 Hazardous function operation prevention** Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function. **Section 3.3.6.2.2.3 Loss of input or failure** Loss of input or failure of the monitor shall be identifiable. **3.3.6.2.2.4 Launch site availability** Monitoring shall be available to the launch site when necessary to assure safe ground operations. **3.3.6.2.2.5 Flight crew availability** Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

203.2	Substantiating Failure Tolerance Payloads must be designed so as to allow substantiation of safing by the Orbiter flight crew or ground crew prior to retrieval and while the payload is still a safe distance from the Orbiter. By direct or indirect means, it must be substantiated that catastrophic hazardous functions are at lest two-failure tolerant. Specific plans to be used to determine the safe status of a retrievable payload must be approved by the NSTS.	**SSP 50021** **Section 3.3.6.2.2 Monitors.** **Section 3.3.6.2.2.1 Status information** Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device. **Section 3.3.6.2.2.2 Hazardous function operation prevention** Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function. **Section 3.3.6.2.2.3 Loss of input or failure** Loss of input or failure of the monitor shall be identifiable. **3.3.6.2.2.4 Launch site availability** Monitoring shall be available to the launch site when necessary to assure safe ground operations. **3.3.6.2.2.5 Flight crew availability** Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

203.3	Monitoring After retrieval, the monitoring requirements of paragraphs 201.1c and 201.3 will apply.	**SSP 50021** **Section 3.3.6.2.3 Near-real time monitoring.** Near-real time monitoring (See 6.1) of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, "Respond to Loss of Function". The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard. **Section 3.3.6.1.5.2 Loss of function resulting in catastrophic hazards** Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels. a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function. b. The function shall be monitored and controlled in accordance with the ISS capabilities "Monitor System Status" and "Respond to Loss of Function".
203.4	Certification Prior to me NSTS retrieval or revisit mission, the payload organization must certify the safety of the payload. This certification must be based upon a hazard analysis that considers the effect of the current condition of the payload (including the impact of all anomalies) during all subsequent flight and ground operations with the STS.	**N/A; Certification intended for payloads not previousy designed/certified to NHB 1700.7**

204	HAZARD DETECTION AND SAFING The need for hazard detection and safing by the flight crew to control time-critical hazards will be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available. When implemented, these functions will be capable of being tested for proper operations during both ground and flight phases and shall use existing Orbiter systems for fault detection and annunciation. Likewise, payload designs should be such that real-time monitoring is not required to maintain control of hazardous functions. With NSTS approval, real-time monitoring and hazard detection and safing may be utilized to support control of hazardous functions provided that adequate crew response time is available and acceptable safing procedures are developed.	**SSP 50021** **Section 3.3.6.2.2 Monitors.** **Section 3.3.6.2.2.1 Status information** Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device. **Section 3.3.6.2.2.2 Hazardous function operation prevention** Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function. **Section 3.3.6.2.2.3 Loss of input or failure** Loss of input or failure of the monitor shall be identifiable. **3.3.6.2.2.4 Launch site availability** Monitoring shall be available to the launch site when necessary to assure safe ground operations. **3.3.6.2.2.5 Flight crew availability** Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

205	CONTINGENCY RETURN AND RAPID SAFING All payloads must be safe for aborts and contingency return and shall include design provisions for rapid safing. Hazard controls may include deployment, jettison or design provisions to change the configuration of the payload.	**SSP 50021** **Section 3.3.6.13.5 Contingency Return and Rapid Safing.** The <End Item> shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop. For emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes. For a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements apply to <End Item> hardware with direct interfaces with the Orbiter: **Section 3.3.6.13.5.1 Emergency deorbit** The <End Item> hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-<End Item> hardware operations. **Section 3.3.6.13.5.2 Next primary landing site contingency deorbit** The <End Item> hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency deorbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-<End Item> hardware operations.
206	FAILURE PROPAGATION The design shall preclude propagation of failures from the payload to the environment outside the payload.	**End Item Boilerplate** **3.2.1.1 Failure propagation.** A single failure of an Orbital Replaceable Unit (ORU) in a functional path within the <End Item> shall not induce any other failures external to the failed ORU.
207	REDUNDANCY SEPARATION Safety-critical redundant subsystems shall be separated by the maximum practical distance, or otherwise protected, to ensure that an unexpected event that damages one is not likely to prevent the others from performing the function. All redundant functions that are required to prevent a catastrophic hazard must not be routed through a single connector.	**End Item Boilerplate** **3.2.1.2 Separation of redundant paths.** Alternate or redundant functional paths shall be separated or protected such that any single credible event which causes the loss of one functional path will not result in the loss of the redundant functional path(s).
208	STRUCTURES	**Title**

208.1	Structural Design The structural design shall provide ultimate factors of safety equal to or greater than 1.4 for all STS mission phases except emergency landing. This includes loads incurred during payload and Orbiter operations for all payload configurations or while changing configuration as specified in the PIP. Verification of design compliance shall be in accordance with NSTS 14046. When failure of structure can result in a catastrophic event, the design shall be based on fracture control procedures to prevent structural failure because of the initiation or propagation of flaw or crack-like defects during fabrication, testing, and service life. Requirements for fracture control are specified in NHB 8071.1.	**SSP 30559, Structural Design and Verification Requirements** **Table 3.3.1-1 Factors of Safety for Test Verified Structure** **3.1.3 STRENGTH AND STIFFNESS** Space Station structure shall have adequate strength and stiffness in all necessary configurations and stages, to support ultimate load without failure. Detrimental deformation shall not occur at limit loads imposed during Shuttle transportation and on-orbit operations, or during proof or acceptance testing. All flight primary structure shall be designed to be either fail-safe, have safe-life, or be a low risk fracture part as defined in SSP 30558, Fracture Control Requirements for Space Station. **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document. **4.1.3.1 STRUCTURAL VERIFICATION FOR SPACE TRANSPORTATION SYSTEM LOADS** The Space Station structural design and verification requirements for the transport phases to and from orbit shall be consistent with the requirements for Shuttle payloads specified in NSTS 14046. ISS elements shall be verified by test and/or analysis to the ascent vibro-acoustic environment defined in ICD 2-19001.

208.2	Emergency Landing Loads The structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in the ICD's between the Orbiter and the payload. Structural verification for these loads may be certified by analysis only.	**SSP 30559, Structural Design and Verification Requirements** **3.2.1 SHUTTLE PAYLOAD CONFIGURATION DESIGN LOADS** For lift-off, ascent, on orbit, descent, landing, and emergency landing using Shuttle, Space Station structure shall be designed to maintain required functionality and positive margins when subjected to all static and dynamic loads and thermal environments as defined in NSTS 07700, Volume XIV, Space Shuttle System Payload Accommodations, and ICD 2-19001, Shuttle Orbiter/Cargo Standard Interfaces. **3.3.2.1 Emergency Landing** The structural design shall comply with the ultimate design load factors for emergency landing loads that are specified in the ICDs between the Orbiter and the payload. Structural verification for these loads may be certified by analysis only.
208.3	Stress Corrosion Materials used in the design of payload structures, support bracketry, and mounting hardware shall be rated for resistance to stress corrosion cracking (SCC) in accordance with the tables in MSFC-HDBK-527/JSC 09604 and MSFC-SPEC-522. Alloys with high resistance to SCC shall be used whenever possible and do not require NSTS approval. When failure of a part made from a moderate or low resistance alloy could result in a critical or catastrophic hazard, a Material Usage Agreement that includes a Stress Corrosion Evaluation Form from MSFC-HDBK-527/JSC 09604 must be attached to the applicable stress corrosion hazard report contained in the safety assessment report (see paragraph 301). When failure of a part made from a moderate or low resistance alloy would not result in a hazard, rationale to support the non-hazard assessment must be included in the stress corrosion hazard report. Approval of the hazard report shall constitute NSTS approval for the use of the alloy in the documented applications. Controls that are required to prevent SCC of components after manufacturing shall be identified in the hazard report and closure shall be documented in the verification log (see paragraph 214.2) prior to flight.	**SSP 30558, Fracture Control Requirements for Space Station** **4.2.4.2.1 Remote Possibility of Significant Crack Like Defects** Assurance against the presence of a significant crack-like defect shall be achieved by compliance with the following criteria: a. The part shall be fabricated from a well-characterized metal which is not sensitive to stress corrosion cracking as defined in MSFC-SPEC-522B, or MSFC-HDBK-527/JSC 09604. If other than Table I or A-rated materials as classified respectively in these documents must be used, suitability for the specific application shall be documented by a Materials Usage Agreement (MUA). MUA forms contained in the cited documents, or equivalent, shall be used. **SSP 30233 Space Station Requirements for Material and Processes** 4.1 MSFC-SPEC-522B, Design for Controlling Stress Corrosion Cracking Criteria shall be used to select metallic material to control stress corrosion cracking.

208.4	Pressure System The maximum design pressure (MDP) for a pressurized system shall be the highest pressure defined by maximum relief pressure, maximum regulator pressure or maximum temperature. Transient pressures shall be considered. Design factors of safety shall apply to MDP. Where pressure regulators, relief devices, and/or a thermal control system (e.g., heaters) are used to control pressure, collectively they must be two-fault tolerant from causing the pressure to exceed the MDP of the system. Pressure integrity shall be verified at the system level.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.2 Pressure System Components** 4.4.2.1 Pressure system components (or equipment) not meeting the definition of pressure vessels given in Appendix B, shall be considered fracture critical if they contain hazardous fluids or if loss of pressurization would result in a catastrophic hazard. All fusion weld joints on Fracture Critical components shall be inspected using a qualified NDE method. In instances where NDE is not feasible, or is incapable of being dealt with successfully, the manufacturer will employ a verification by sampling procedure for establishing the quality of uninspectable welds. This option requires NASA approval. Cracks or any other type of flaw indication not meeting specification requirements shall be cause for rejection of these components. Safe-life analysis is not required for fracture critical pressurized lines, fittings and components which are proof tested to the factor of safety requirements of SSP 30559, Structural Design and Verification Requirements, section 3.3. In addition to proof testing of parts during individual acceptance, pressure integrity shall be verified at the system level. **Appendix B Glossary** **Maximum Design Pressure** The Maximum Design Pressure (MDP) for a pressurized system is the highest pressure defined by the maximum relief pressure, maximum regulator pressure, maximum temperature, and transient pressure excursions. **SSP 30559, Structural Design and Verification Requirements** **3.1.9 Design Requirements for Pressure System**
208.4a	Pressure Vessels. Pressure vessels shall comply with the pressure vessel requirements of MIL-STD-1522A (including revisions as of December 1984) as modified by the paragraphs (1), (2), (3), (4) and (5) below. Particular attention shall be given to insure compatibility of vessel materials with fluids used in cleaning, test, and operation. Data requirements for pressure vessels are listed in NSTS 13830.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1 Pressure Vessels** **4.4.1.1** Pressure vessels, as defined in Appendix B, shall comply with requirements in Sections 4 and 5 of MIL-STD-1522A, Standard General Requirements for Safe Design and Operations of Pressurized Middile and Space Systems, including revisions as of December 1984, modified as follows:

208.4a(1)	Approach ”B” of figure 2 is not acceptable.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1. (b)** Approach “B” of Figure 2 in MIL-STD-1522A is not acceptable and shall not be used.
208.4a(2)	In addition to other required analyses, composite pressure vessels shall be assessed for adequate stress rupture life.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1. (f)** In addition to other required analyses, composite pressure vessels shall be assessed for adequate stress rupture life and effects of atomic oxygen.
208.4a(3)	Nondestructive evaluation (NDE) of pressure vessels shall include inspection of welds after proof testing.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1. (g)** NDE of safe life pressure vessels shall include inspection of welds before and after proof testing.
208.4a(4)	MDP as defined above (see paragraph 208.4) shall be substituted for all reference to maximum expected operating pressure (MEOP).	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1. (d)** MDP as defined in Appendix B, shall be substituted for all reference to maximum expected operating pressure in MIL-STD-1522A.
208.4a(5)	A proof test of each flight pressure vessel to a minimum of 1.5 x MDP and a fatigue analysis showing a minimum of 10 design lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of this document and MIL-STD-1522A, Approach A.	**SSP 30558, Fracture Control Requirements for Space Station** **4.4.1. (j)** For low cycle applications a proof test of each flight pressure vessel to a minimum of 1.5 times MDP and a fatigue analysis showing the greater of 500 pressure cycles or 10 lifetimes may be used in lieu of testing a certification vessel to qualify a vessel design that in all other respects meets the requirements of SSP 30559 and MIL-STD-1522A, Approach A.
208.4b	Dewars. Dewar/cryostat systems are a special category of pressurized vessels because of unique structural design and performance requirements. Pressure containers in such systems shall be subject to the requirements for pressure vessels specified in paragraphs 208.4 and 208.4a as supplemented by the requirements of this section.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 Dewars** Dewar/cryostat systems shall be designed in accordance with the pressure vessel requirements in SSP 30558, section 4.4. and the following:

208.4b(1)	Pressure containers shall be leak-before-bust (LBB) designs were possible as determined by fracture mechanics analysis. Containers of hazardous fluids and all non-LBB designs must employ a fracture mechanics safe-life approach to assure safety of operation.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (a)** Pressure containers shall be leak-before-bust (LBB) designs were possible as determined by fracture mechanics analysis. Containers of hazardous fluids and all non-LBB designs must employ a fracture mechanics safe-life approach to assure safety of operation.
208.4b(2)	MDP of the pressure container shall be as determined in paragraphs 208.4 or the pressure achieved under maximum venting conditions whichever is higher. Relief devices must be sized for full flow at MDP.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (b)** MDP assessment for the pressure container shall envelop the pressure achieved under maximum venting conditions.
208.4b(3)	Outer shells (i.e., vacuum jackets) shall have pressure relief capability to preclude rupture in the event of pressure container leakage. If pressure containers do not vent external to the dewar but instead vent into the volume contained by the outer shell, the outer shell relief devices must be capable of venting at a rate to release full flow without outer shell rupture. Relief devices must be redundant and individually capable of full flow.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (c)** Outer shells (i.e., vacuum jackets) shall have pressure relief capability to preclude rupture in the event of pressure container leakage. If pressure containers do not vent external to the dewar but instead vent into the volume contained by the outer shell, the outer shell relief devices must be capable of venting at a rate to release full flow without outer shell rupture. Relief devices must be redundant and individually capable of full flow.
208.4b(4)	Pressure relief devices which limit maximum design pressure must be certified to operate at the required conditions of use. Certification shall include testing of the same part number from the flight lot under the expected use conditions.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (d)** Pressure relief devices which limit maximum design pressure must be certified to operate at the required conditions of use. Certification shall include testing of the same part number from the flight lot under the expected use conditions.
208.4b(5)	Nonhazardous fluids may be vented into the cargo bay if analysis shows that a worst case credible volume release will not affect the structural integrity or thermal capability of the Orbiter.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (e)** Nonhazardous fluids may be vented into the cargo bay if analysis shows that a worst case credible volume release will not affect the structural integrity or thermal capability of the Orbiter.
208.4b(6)	The reproof test factor for each flight pressure container shall be a minimum of 1.1 times MDP. Qualification bust and pressure cycle testing is not required if all the requirements of paragraphs 208.4, 208.4a and 208.4b are met. The structural integrity for external load environments must be demonstrated in accordance with NSTS 14046.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.3 (f)** The reproof test factor for each flight pressure container shall be a minimum of 1.1 times MDP. Qualification bust and pressure cycle testing is not required if all the requirements of paragraphs 3.1.9 are met. The structural integrity for external load environments must be demonstrated in accordance with NSTS 14046.

208.4c	Pressurized Lines, Fittings, and Components	**SSP 30559, Structural Design and Verification Requirements** **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document. **Table 3.3.1-1 Factors of Safety for Test Verified Structure**
208.4c(1)	Pressurized lines and fittings with less than a 1.5-inch outside diameter and all flex-houses shall have an ultimate factor of safety equal to or greater than 4.0. Lines and fittings with a 1.5-inch or greater outside diameter shall have an ultimate factor of safety equal to or greater than 1.5.	**SSP 30559, Structural Design and Verification Requirements** **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document. **Table 3.3.1-1 Factors of Safety for Test Verified Structure**
208.4c(2)	All line-installed bellows and all heat pipes shall have an ultimate safety factor equal to or greater than 2.5.	**SSP 30559, Structural Design and Verification Requirements** **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document. **Table 3.3.1-1 Factors of Safety for Test Verified Structure**
208.4c(3)	Other components (e.g., valves, filters, regulators, sensors, etc.) and their internal parts (i.e., bellows, diaphragms, etc.) which are exposed to system pressure shall have an ultimate factor of safety equal to or greater than 2.5.	**SSP 30559, Structural Design and Verification Requirements** **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document. **Table 3.3.1-1 Factors of Safety for Test Verified Structure**

208.4c(4)	Secondary compartments or volumes that are integral or attached by design to the above parts and which can become pressurized as a result of a credible single barrier failure must be designed for safety consistent with structural requirements. These compartments shall have a minimum safety factor of 1.5 based on MDP. If external leakage would not present a catastrophic hazard to the Orbiter, the secondary volume must either be vented or equipped with a relief provision in lieu of designing for system pressure.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.4 Secondary Volumes** Secondary compartments or volumes that are integral or attached by design to pressure system components and which can become pressurized as a result of a credible single barrier failure shall be designed for safety consistent with structural requirements. Redundant seals in series which have been acceptance pressure tested individually prior to flight shall not be considered credible single barrier failure. Failures of structural parts such as pressure lines and tanks, and properly designed and tested welded or brazed joints shall not be considered single barrier failures. In order to be classified as non-credible failure, the item shall be designed for a safety factor of 2.5 on the MDP, and shall be certified for all operating environments including fatigue conditions. If extenal leakage would not present a catastrophic hazard, the secondary volume shall either be vented or equipped with a relief provision in lieu of designing for system pressure.
208.4d	Flow Induced Vibration. Flexible hoses and bellows shall be designed to exclude flow induced vibrations which could result in a catastrophic hazard to the STS.	**SSP 30559, Structural Design and Verification Requirements** **3.1.9.5 Flow Induced Vibration** All flexible hoses and bellows shall be designed to exclude or minimize flow induced vibrations in accordance with MSFC-DWG-20M02540. Certification of hardware shall be in accordance with NSTS 08123. When certification by test is required, requirements in MSFC-SPEC-626 shall apply.
208.5	Sealed Compartments Payload sealed compartments within a habitable volume, including containers which present a safety hazard if rupture occurs, shall be capable of withstanding the maximum pressure differential associated with emergency depressurization of the habitable volume. Payloads located in any other region of the Orbiter shall be designed to withstand the decompression and repressurization environments associated with ascent or decent.	**End Item Boilerplate** **3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance.** **3.3.6.11.2.1 Pressure differential tolerance** <End Item> equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard.

209	MATERIALS MSFC-HDBK-527/JSC 09604 contains a listing of materials (both metals and nonmetals) with a "rating" indicating acceptability for each material's characteristic. For materials which create potential hazardous situations as described in the paragraphs below and for which no prior NASA test data or rating exists, the payload organization shall present other test results for NSTS review or request assistance from the NSTS in conducting applicable tests. The payload material requirements for hazardous materials, flammability, and offgassing are as follows:	**SSP 30233 Space Station Requirements for Material and Processes** Scope
209.1	Hazardous Materials Hazardous materials shall not be released or ejected in or near the Orbiter. During exposure to all STS environments, hazardous fluid systems must contain the fluids unless the use of the Orbiter vent/dump provisions has been negotiated with the NSTS.	**SSP 50021** **Section 3.3.6.13.9 Orbiter vent/dump provisions** **Section 3.3.6.13.9.1 Release or ejection of hazardous material** <End Item> hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS. **Section 3.3.6.13.9.2 Fluid system containment** <End Item> shall be designed to contain both hazardous and nonhazardous fluids when in the presence of the Orbiter.
209.1a	Fluid Systems. Particular attention shall be given to materials used in systems containing hazardous fluids. These hazardous fluids include gaseous oxygen, liquid oxygen, fuels, oxidizers, and other fluids that could chemically or physically degrade the system or cause an exothermic reaction. Those materials within the system exposed to oxygen (liquid and gaseous), both directly and by a credible single barrier failure, must meet the requirements of NHB 8060.1 at MDP and temperature. Materials within the system exposed to other hazardous fluids, both directly and by a credible single barrier. failure, must pass the fluid compatibility requirements of NHB 8060.1 at MDP and temperature. The payload supplier's compatibility data on hazardous fluids may be used to accept materials in this category if approved by the NSTS.	**SSP 30233 Space Station Requirements for Material and Processes** **4.1** Metallic materials shall meet the requriements of NASA-NHB-8060.1C, Flammability, Odor, and Offgassing Compatibility Requirements and Test Procedures for Materials in Environmnents that Support Combustion, as a minimum. **4.2** As a general requirements for all nonmetallic materials, the contractor shall obtain data or analyses as necessary to meet the requirements of NHB 8060.1C. The toxic Hazard Index (T) for materials/assemblies shall be calculated suing the methods defined in Test 7. SMAC values shall be selected from either NHB 8060.1B, Appendix D or MAPTIS. **SSP 50021** **Section 3.3.12.5 Fluid handling requirements.** **Section 3.3.12.5.1 Fluid handling requirements.** Fluids shall comply with SSP 30573.

209.1b	Chemical Releases. The use of chemicals which would create a toxicity problem (including irritation to skin or eyes) or cause a hazard to STS hardware if released should be avoided. If use of such chemicals cannot be avoided, adequate containment shall be provided by the use of an approved pressure vessel as defined in paragraph 208.4 or the use of two or three redundantly sealed containers, depending on the toxicological hazard for a chemical with a vapor pressure below 15 psia. The payload organization must assure that each level of containment will not leak under the maximum use conditions (i.e., vibration, temperature, pressure, etc.). Mercury is an example of such a chemical, since it produces toxic vapors and can amalgamate with metals or metal alloys used in spacecraft hardware. Documentation of chemical usage, along with the containment methods, will be supplied for review and approval.	**SSP 50021** **Section 3.3.6.4 Hazardous materials.** **Section 3.3.6.4.1 Hazardous fluid containment failure tolerance.** Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558. **Section 3.3.6.4.2 Storage of Hazardous Chemicals.** Hazardous experiment payload chemicals/materials shall be stored only in International Standard Payload Racks (ISPRs) located in U.S. Laboratory or Logistics Modules.
209.2	Flammable Materials A payload must not constitute an uncontrolled fire hazard to the STS or other payloads. The minimum use of flammable materials shall be the preferred means of hazard reduction. The determination of flammability shall be in accordance with NHB 8060.1. Guidelines for the conduct of flammability assessments are provided in NSTS 22648. A flammability assessment shall be documented in accordance with NSTS 13830.	**SSP 50021** **Section 3.2.11.1 Materials and Processes** Materials and processes shall be selected in accordance with SSP 30233. **SSP 30233 Space Station Requirements for Material and Processes** **4.1** Metallic materials shall meet the requriements of NASA-NHB-8060.1C, Flammability, Odor, and Offgassing Compatibility Requirements and Test Procedures for Materials in Environmnents that Support Combustion, as a minimum. **4.2** As a general requirements for all nonmetallic materials, the contractor shall obtain data or analyses as necessary to meet the requirements of NHB 8060.1C. The toxic Hazard Index (T) for materials/assemblies shall be calculated suing the methods defined in Test 7. SMAC values shall be selected from either NHB 8060.1B, Appendix D or MAPTIS.

209.2a	Orbiter Cabin. Materials used in the Orbiter cabin must be tested in accordance with NHB 8060.1 at the use condition of 10.2 psi total pressure and 30 percent oxygen concentration (worst case Orbiter cabin condition). When flammable materials are used in quantities where the weight or surface area is greater than 0.1 pounds or 10 square inches respectively, the methods of control of flame propagation must be described in the flammability assessment report.	**SSP 50021** **Section 3.2.9.1 Materials and Processes** Materials and processes shall be selected in accordance with SSP 30233.
209.2b	Other Habitable Areas. Materials used in habitable areas other than the Orbiter cabin shall be tested in accordance with NHB 8060.1 in the worst case atmosphere (i.e., oxygen concentration). Propagation path considerations of paragraph 209.2a apply.	**SSP 50021** **Section 3.2.11.1 Materials and Processes** Materials and processes shall be selected in accordance with SSP 30233.
209.2c	Outside Habitable Areas. Materials used outside the Orbiter cabin shall be evaluated for flammability in an air environment at 14.7 psi. Propagation path considerations of NSTS 22648 apply for material usages of greater than 1 pound and/or dimensions exceeding 12 inches.	**SSP 50021** **Section 3.2.11.1 Materials and Processes** Materials and processes shall be selected in accordance with SSP 30233.
209.3	Material Offgassing in Habitable Areas Usage of materials which produce toxic levels of offgassing products shall be avoided in habitable areas. Payload elements going into such areas are required to be subjected to offgassing tests (black-box levels) for safety validation prior to integration with STS elements. Rigorous material control to insure that all selected materials have acceptable offgassing characteristics is a negotiable alternative to black-box level testing. The offgassing test specified in NHB 8060.1 or an NSTS approved equivalent shall be used for the black-box level offgassing test. The document MSFC-HDBK-527/JSC 09604 contains a listing of materials and black boxes that have been subjected to offgassing tests.	**SSP 50021** **Section 3.2.11.1 Materials and Processes** Materials and processes shall be selected in accordance with SSP 30233. **SSP 30233 Space Station Requirements for Material and Processes** **4.1** Metallic materials shall meet the requriements of NASA-NHB-8060.1C, Flammability, Odor, and Offgassing Compatibility Requirements and Test Procedures for Materials in Environmnents that Support Combustion, as a minimum. **4.2** As a general requirements for all nonmetallic materials, the contractor shall obtain data or analyses as necessary to meet the requirements of NHB 8060.1C. The toxic Hazard Index (T) for materials/assemblies shall be calculated suing the methods defined in Test 7. SMAC values shall be selected from either NHB 8060.1B, Appendix D or MAPTIS.

210	PYROTECHNICS If premature firing of a pyrotechnic device or failure of a pyrotechnic device to fire will cause a hazard to the STS, the pyrotechnic subsystem and devices shall meet the design and test requirements of MIL-STD-1512.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
210.1	Initiators NASA Standard Initiators (NSI's) should be used for functions where premature firing is catastrophic such as deployment from the Orbiter, stage separation, and SRTM ignition. Alternate equivalent initiator designs will be considered on a case-by-case basis and will require approval by the NSTS. When alternate initiators are used, it must be thoroughly demonstrated that such initiators are not susceptible to premature firing from electrostatic discharge. This demonstration will not be required: if the pyrotechnic subsystem contains an S&A device that provides a mechanical interrupt of the pyrotechnic train immediately downstream of the initiator; and the S&A device stays in the "SAFE" position until after the payload has been deployed and reaches a safe distance from the Orbiter. When the S&A exception does not apply, alternate initiators must meet the following minimum criteria and demonstration requirements.	**SSP 50021** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions.

210.1a	Flight Unit Acceptance Test. All the initiators in the lot from which the flight initiators are taken must meet the static discharge sensitivity test requirement of Method 205 of MIL-STD-1512 without a resistor in the test firing circuit. Single bridgewire initiators shall not be subjected to the pin-to-pin test.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
210.1b	Design Configuration. Single bridgewire initiators are preferred. If dual bridgewire initiators are used, the electrostatic discharge sensitivity test described in paragraph 210.1a shall be conducted between bridgewires as well as bridgewire-to-case (three tests). It is preferred that the electrostatic protection feature be hermetically sealed to insure protection stability under all environments.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.

210.1c	Design Verification. If a hermetic seal is not used to provide environmental stability, test or analysis must demonstrate that the electrostatic discharge protection exists under all environments including space vacuum. If is also required to demonstrate that the above flight unit acceptance test does not degrade the protection features of the unit under subsequent exposure to electrostatic discharge or other phenomena which could cause premature firing.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
210.2	Pyrotechnic Operated Devices	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.

210.2a	Debris Protection. Pyrotechnic devices that are to be operated in the Orbiter or that do not meet the criteria of this document to prevent inadvertent operation, shall be designed to preclude hazards due to effects of shock, debris, and hot gasses resulting from operation. Such devices shall be subjected to a "locked-shut" safety demonstration test (i.e., a test to demonstrate the capability of the devices to safety withstand internal pressures generated in operation with the moveable part restrained in its initial position).	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
210.2b	Must Function Safety Critical Devices. Where failure to operate will cause a catastrophic hazard, pyrotechnic operated devices shall be designed, controlled inspected, and certified to criteria equivalent to those specified in NSTS 08060. The data required for NSTS review are identified in NSTS 13830. If the device is used in a redundant application where the hazard is being controlled by the use of multiple independent methods, then in lieu of demonstrating compliance with criteria equivalent to NSTS 08060, sufficient margin to assure operation must be demonstrated. When required, pyrotechnic operated devices shall demonstrate performance margin using a single charge or cartridge loaded with 85 percent (by weight) of the minimum allowable charge or other equivalent margin demonstrations.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.

210.2c	Electrical Connection. Payloads with pyrotechnic devices which if prematurely fired may cause injury to people or damage to property shall be designed such that these devices can be electrically connected in the Orbiter after all payload/Orbiter electrical interface verification tests have been completed. Ordnance circuitry must be verified safe prior to connection of pyrotechnical devices. Exceptions to this require specific approval of the Launch Site Safety Office.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
210.3	Traceability The payload organization shall furnish the NSTS a list of all safety critical pyrotechnic initiators installed or to be installed on the payload, giving the function to be performed, the part number, the lot number , and the serial number.	**SSP 50021** **Section 3.3.6.5 Pyrotechnics.** **Section 3.3.6.5.1 Pyrotechnics for USOS application.** **Section 3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **Section 3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **Section 3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
211	DESTRUCT SYSTEMS Destruct systems will be used only when approved by the NSTS and must comply with the requirements of paragraphs 200, 201,. 202, 204, and 210.	**N/A No Destruct System on ISS**
212	RADIATION	**N/A on ISS (3.3.6.6)**

212.1	Ionizing Radiation Payloads containing or using radioactive materials or that generate ionizing radiation shall be identified and approval obtained for their use. Descriptive data shall be provided in accordance with NSTS 13830. Major radioactive sources require approval by the Interagency Nuclear Safety Review Panel through the NASA coordinator of the panel. DOD payloads involving radioactive materials will be processed through their own established procedures. Radioactive materials shall comply with appropriate license requirements at the planned launch and landing sites.	**SSP 50021** **Section**
212.2	Nonionizing Radiation Payloads shall not emit electromagnetic radiation which presents a hazard. The payload design shall be compatible with the payload bay environment as specified in the ICD between the payload and the Orbiter.	**SSP 50021** **Section 3.3.6.6.1 Nonionizing Radiation.** The <End Item> shall limit the levels of nonionizing radiation of the <End Item> in accordance with SSP 50005, paragraphs 5.7.3.2 and 5.7.3.2.1 to provide personnel protection.
212.3	Lasers Lasers used on STS payloads shall be designed and operated in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1.	**SSP 50021** **Section 3.3.6.7.1 Lasers** Lasers used on <End Item>s shall be in accordance with American National Standard for Safe Use of Lasers, ANSI-Z-136.1.
213	ELECTRICAL SYSTEMS	**Title**

213.1	General Electrical power distribution circuitry shall be designed so that faults internal to the payload do not damage STS circuitry and do not create ignition sources for adjacent Orbiter or payload flammable materials. Payload circuits should contain protection devices sized to prevent undamaged wire segments from exceeding the temperature rating of the wire insulation while being subjected to a current at the ultimate trip limit of the protection device for an indefinite period of time. Bent pins or conductive contamination in an electrical connector will not be considered a credible failure mode if a post-mate functional verification is performed to assure that shorts between adjacent connector pins or from pins to connector shell do not exist. If this test cannot be performed, then the electrical design must insure that any pin if bent prior to or during connector mating cannot invalidate more than one inhibit and that conductive contamination is precluded by proper inspection procedures.	**SSP 50021** **Section 3.3.6.8 Electrical Safety** **Section 3.3.6.8.1 Electrical power circuit overloads.** **Section 3.3.6.8.1.1 Circuit overload protection** Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits. **Section 3.3.6.8.1.2 Protective device sizing** Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded. **Section 3.3.6.8.1.3 Bent pin or conductive contamination** **a.** <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function. **b.** Conductive contamination as a similar cause shall be precluded. **3.3.6.8.2 Crew protection for electrical shock.** The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3. **3.3.6.8.3 Reapplication of power.** The <End Item> shall provide local control of interruption and reapplication of power to each IVA maintenance area.

213.2	Batteries Batteries use don STS payloads shall be designed to control applicable hazards caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of overtemperature, shorts, reverse current, cell reversal, leakage, cell grounds, and overpressure. Safety guidelines for STS payload batteries are contained n NSTS 20793. Since lithium batteries have uniquely hazardous failure modes, their use is discouraged where the use of other types of cells is feasible. When lithium batteries are used, the NSTS will require extensive testing and analyses to demonstrate their safety under all applicable failure modes.	**SSP 50021** **Section 3.3.6.8.4 Batteries.** <End Item> batteries which can pose a hazard shall be designed in accordance with NSTS 20793.
213.3	Lightning Payload electrical circuits may be subjected to the electromagnetic fields described in NSTS 078700, Volume XIV, Attachment 1 (ICD-2-19001) due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall be hardened against the environment or insensitive devices (relays) shall be added to control the hazard.	**SSP 50021** **Section 3.3.6.13.8 Lightning protection** <End Item> electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard.
214	VERIFICATION Test, analysis, and inspection are common techniques for verification of design features used to control potential hazards. The successful completion of the safety process will require positive feedback of completion results for all verification items associated with a given hazard. Reporting of results by procedure/report number and date is required.	**Verification is identified for each cited "shall" statement in section 4 of the specifications.**
214.1	Mandatory Inspection Points (MIP's) When procedures and/or processes are critical steps in controlling a hazard and the procedure and/or process results will not be independently verified by subsequent test or inspection, it will be necessary to insure the procedure/process is independently verified in real-time. Critical procedure/process steps must be identified in the appropriate hazard report as MIP's requiring independent observation.	**Will be provided per MOD documentation.**
214.2	Verification Tracking Log A payload safety verification tracking log (see NSTS 13830) is required to properly status the completion steps associated with hazard report verification items.	**Verification Tracking Log is required in the Data Requirement from NASA to Boeing (SM02).**
215	HAZARDOUS OPERATIONS	**Title**

215.1	Hazard Identification The payload organization shall assess all payload flight and ground operations and determine their hazard potential to the STS. The hazardous operations identified shall be assessed in the applicable flight or ground safety assessment report.	**Hazard identification is required per NASA Statement of Work.**
215.2	Exposure to Risk STS exposure to increased risk as a result of ground or flight operations shall be minimized. Those ground operations (e.g., arm plug installation in a payload pyrotechnic system, final ordnance connection, radioisotope thermoelectric generator (RTG) installation, etc.) which place the payload in a configuration of increased hazard potential shall be accomplished as late as practicable during the payload processing flow at the launch site.	

215.3	Access Payloads shall be designed such that any required access to hardware during flight or ground operations can be accomplished with minimum risk to personnel.	**SSP 50021** **Section 3.3.6.1.7 Safety interlocks.** Safety interlocks shall be provided to prevent unsafe operations when access to <End Item> equipment is required for maintenance. **Section 3.3.6.14 Ground interfaces and services - Space Shuttle launch** Hazards shall not be created due to the inaccessibility of flight hardware such as:. **Section 3.3.6.14.a Moving parts** Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices. **Section 3.3.6.14.b Equipment requiring adjustment** Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable. **Section 3.3.6.14.c Ignition of adjacent materials** Electrical equipment shall not cause ignition of adjacent materials. **Section 3.3.6.14.d Accidental contact with electrical equipment** Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.
216	SERIES PAYLOADS AND REFLOWN HARDWARE ”Reflown hardware” are payloads or elements of payloads which are made up of hardware items that have already physically flown on the STS and are being manifested for reflight. ”Series payloads” are payloads or elements of payloads which are of the same or similar design to previo<End Item>y flown STS payloads.	**Definition**

216.1	Recertification of Safety Series payloads and reflown hardware must be recertified safe and must meet all the safety requirements of this document. Caution should be exercised in the use of previous safety verification data for the new usage.	**SSP 30599 paragraph 7.0**
216.2	Previous Mission Safety Deficiencies All anomalies during the previous payload missions must be assessed for safety impact. Those anomalies affecting safety critical systems must be reported and corrected. Rationale supporting continued use of the affected design, operations or hardware must be provided for NSTS approval.	**SSP 30599 paragraph 7.0**
216.3	Limited Life Items All safety critical age sensitive equipment must be refurbished or replaced to meet the requirements of the new STS mission.	**SSP 30599 paragraph 7.0**
216.4	Refurbishment Safety impact of any changes, maintenance or refurbishment made to the hardware or operating procedures must be assessed and reported in the safety assessment reviews (paragraph 304). Hardware changes include changes in the design of the payload, changes of the materials of construction, changes in sample materials that may be processed by the payload, etc.	**SSP 30599 paragraph 7.0**
216.5	Safety Waivers and Deviations The acceptance rationale for all deviations from the previous flight must be revalidated by the payload organization. Waivered conditions from the previous STS flight must be corrected.	**SSP 30599 paragraph 7.0**

217	EXTRAVEHICULAR ACTIVITY (EVA) All payload requirements for EVA must be defined and documented in the PIP. Any agreed to EVA task used to satisfy the failure tolerance criteria of this document can be used only as a third level of protection to safe a payload. Payload organizations which plan to use crew EVA for mission enhancement, mission success, or safety critical payload operations will comply with the requirements of NSTS 07700, Volume XIV, Appendix 7.	**SSP 50021** **Section 3.3.6.12 Human engineering safety** **Section 3.3.6.12.1 Internal volume touch temperature.** **Section 3.3.6.12.1.1 Continuous contact - high temperature** Surfaces which are subject to continuous contact with crewmember bare skin and whose temperature exceeds 113 degrees Fahrenheit, shall be provided with guards or insulation to prevent crewmember contact. **Section 3.3.6.12.1.2 Incidental or momentary contact - high temperature** For incidental or momentary contact (30 seconds or less), the following apply: Crewmember warning - Surfaces which are subject to incidental or momentary contact with crewmember bare skin and whose temperatures are between 113 and 122 degrees Fahrenheit shall have warning labels that will alert crewmembers to the temperature levels. Crewmember protection - Surface temperatures which exceed 122 degrees Fahrenheit shall be provided with guards or insulation that prevent crewmember contact. **Section 3.3.6.12.1.3 Internal volume low touch temperature** When surfaces below 39 degrees Fahrenheit which are subject to continuous or incidental contact, are exposed to crewmember bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site. **Section 3.3.6.12.2 External touch temperature.** For crew protection from high or low touch temperature extremes the following apply: **Section 3.3.6.12.2.1 Incidental contact** For incidental contact, temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates as specified in Table 2. **Section 3.3.6.12.2.2 Unlimited contact** For unlimited contact, temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table 3, limit heat transfer rates as specified in Table 2.

217	EXTRAVEHICULAR ACTIVITY (EVA)	**SSP 50021** **Section 3.3.6.12.3 External corner and edge protection.** **Section 3.3.6.12.3.1 Sharp edges** <End Item> equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb. **Section 3.3.6.12.3.2 Thin materials** Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches. **Section 3.3.6.12.3.3 Planned maintenance or storage** Equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.1 **Section 3.3.6.12.4 Internal corner and edge protection.** **Section 3.3.6.12.4.1 Equipment exposed to crew activity** Surfaces of <End Item> equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment. **Section 3.3.6.12.4.2 Equipment exposed only during planned maintenance activities** Corners and edges of material, equipment **or ORUs** which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

217	EXTRAVEHICULAR ACTIVITY (EVA)	**SSP 50021** **Section 3.3.6.12.5 Contingency repressurization.** Controls necessary for restoring a depressurized module to normal operating pressurized conditions shall be capable of being manually operated by an EVA suited crewperson as specified in SSP 50005, paragraph 14.3. **Section 3.3.6.12.6 Latches.** Latches or similar devices shall be designed to prevent entrapment of crewmember appendages. **Section 3.3.6.12.7 Screws and bolts.** Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener. **Section 3.3.6.12.8 Safety Critical Fasteners** Safety critical fasteners shall be designed to prevent inadvertent back out. **Section 3.3.6.12.9 Levers, cranks, hooks and controls.** Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing. **Section 3.3.6.12.10 Burrs.** Exposed surfaces shall be smooth and free of burrs. **Section 3.3.6.12.11 Holes** **Section 3.3.6.12.11.1 Equipment located inside habitable volumes** Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes. **Section 3.3.6.12.11.2 Equipment located outside habitable volumes** Holes (round, slotted, polygonal) in EVA translation hand rails/holds shall be 1.0 inches or greater in diameter.

217	EXTRAVEHICULAR ACTIVITY (EVA)	**SSP 50021** **Section 3.3.6.12.12 Protrusions** Equipment except for translation aids identified in Table 3 shall not protrude into the 50 inch horizontal by 72 inch vertical envelope of the CETA/MT corridor, or the 43 inch horizontal envelope of the primary and secondary translation path. **Section 3.3.6.12.13 Pinch points.** Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crewmember appendages. **Section 3.3.6.12.16 Flexhoses.** Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware. **Section 3.3.6.12.17 Translation routes and established worksites.** For protection from hazards along translation routes and established worksites the following apply: **Section 3.3.6.12.17.1 Primary translation routes and established worksites** **a.** Primary translation routes and established worksites shall not pose a risk to EVA crew. **b.** External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads. **Section 3.3.6.12.17.2 Secondary translation routes and established worksites** External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded and controlled as specified in Table 4. **Section 3.3.6.12.17.3 EVA crewmember contact isolation** <End Item> hardware which cannot be controlled by design features to comply with ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crewmember contact. **Section 3.3.6.12.18 Moving or rotating equipment.** The EVA crewmember shall be protected from moving or rotating equipment.

218	PAYLOAD COMMANDING All hazardous commands that can be sent to the payload shall be identified. Hazardous commands are those that can remove an inhibit to a hazardous function or activate an unpowered hazardous payload system. Failure modes associated with payload flight and ground operations including hardware, software, and procedures used in commanding from payload operations control centers (POCC's) and other ground equipment must be considered in the safety assessment to determine compliance with the requirements of paragraphs 200.1, 201, and 202. NSTS 19943 treats the subject of hazardous commanding and presents the guidelines by which it will be assessed.	
219	FLAMMABLE ATMOSPHERES During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal payload functions shall not cause ignition of a flammable payload bay atmosphere that may result from leakage or ingestion of fluids into the payload bay.	**SSP 50021** **Section 3.3.6.13.6 Flammable Atmosphere.** **Section 3.3.6.13.6.1 Normal functions** During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) <End Item> functions shall not cause ignition of a potential flammable payload bay atmosphere. **Section 3.3.6.13.6.2 Electrical ignition sources** Electrical ignition sources shall not be exposed. **Section 3.3.6.13.6.3 Surface temperatures** Surface temperatures shall be below 352 degrees F. **Section 3.3.6.13.6.4 Conductive surfaces** Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1.
220	CREW HABITABLE PAYLOADS This paragraph establishes additional safety requirements applicable to NSTS crew habitable payloads. A crew habitable payload is defined as a space capsule (spacecraft or module) which when docked or mated with the Orbiter and provided with atmospheric support from Orbiter systems, is capable of supporting intravehicular activity (IVA) in a shirt sleeve environment for a limited period of time. The crew habitable payload may either be an orbiting capsule visited by the Orbiter or a capsule launched and returned within the Orbiter cargo bay.	**N/A**

220.1	Atmosphere	**N/A**
220.1a	Verification of Habitability	**N/A**
220.1a(1)	Offgassing. The payload design shall assure the offgassing load to the internal manned compartment will not exceed the spacecraft maximum allowable concentrations (SMAC's) of atmospheric contaminants specified in JSC 20584 at the time of ingress. All crew habitable payload hardware will be tested for offgassing characteristics according to NHB 8060.1B as required by paragraph 209.3 of this document and will include measurement of the internal atmosphere of a full scale, flight configured payload as a final verification of acceptability. Time periods prior to crew ingress during which the payload does not have active atmospheric contamination control must be considered.	**N/A**
220.1a(2)	Verification for Revisit Missions. Payloads that remain in orbit for extended periods must ensure that the manned compartment is environmentally safe prior to crew ingress during any revisit. Additionally, provisions for sampling of the representative payload internal atmosphere prior to crew ingress shall be provided. Post flight ground analysis of this sample by the NSTS is required prior to the next revisit to determine any unusual gas buildup and the need to define toxic gas detection requirements prior to the subsequent revisit missions.	**N/A**
220.1a(3)	Experiment Leakage. Experiments conducted during manned operations must meet the containment requirements of paragraph 209.1b. Experiment configurations during unmanned operations are not restricted; however, the manned compartment must be environmentally safe for crew ingress during any revisit. Safe conditions for entry may be established by review of the containment design features, proof of adequate atmospheric scrubbing for the chemical involved, vacuum evaluation, use of payload provided equipment capable of detecting toxic chemicals prior to crew exposure, or other techniques suitable for the particular experiment involved.	**N/A**

220.1b	Internal Environment. A safe and habitable internal environment shall be provided within the payload throughout all manned operational phases. The payload system shall provide proper mixing and circulation of the atmosphere to assure adequate atmosphere revitalization by the Orbiter Environmental Control and Life Support Subsystem (ECLSS) and distribution throughout the payload.	**N/A**
220.1c	Cross Contamination. The payload shall be designed so as not to create a contamination hazard in the atmosphere being shared with the Orbiter. The payload shall provide a scrubber and filter system with sufficient capability to cleanse the payload internal atmosphere of the expected vapor and particulate contamination load. SMAC's of atmospheric contaminates are specified in JSC 20584. The scrubber and filter system shall be capable of being activated prior to crew ingress into the payload.	**N/A**
220.1d	Evacuation. The capability to isolate the payload from the Orbiter and non-propulsively vent the payload internal atmosphere shall be provided. The activation of the vent system shall be available to the crew in the Orbiter whenever the payload is attached to the Orbiter.	**N/A**
220.2	Habitability The habitability of the payload directly affects the crewmember's ability to perform efficiently and safely. Payload design features related to habitability shall be compatible with and equivalent to those provided by the Orbiter. NASA-STD-3000 defines guidelines for the design of crew-related systems. NASA-STD-3000 dos not represent requirements imposed by NASA on manned payloads, but rather, is provided to assist payload organizations in identifying desirable habitability subsystem design goals. Specific agreements on habitability design will be developed in the payload integration process. However, if payload environment is jeopardizing crew safety (e.g., affecting crew health, inducing fatigue to the point that safety critical tasks could be affected, interfering with voice communication, etc.), the crew will egress and isolate the payload atmosphere from the Orbiter.	**N/A**

220.2a	Acoustic Noise. The maximum continuous acoustic noise sound pressure level in the payload crew habitable area during manned operations shall not exceed the NR-50 contour of the International Organization of Standardization (ISO) Noise Rating, or the NC-50 contour of the United States Noise Criteria Standard, whichever is higher, except that the noise level in the octave bands of 63 hertz and below is limited to a maximum of 75 dB. The maximum sound pressure level of any narrow band continuous component shall be at least 10 dB less than the broad band sound pressure level of the octave band which contains the component. These acoustic noise limits shall apply to the sound pressure levels produced by the summation of all the individual sound pressure levels from all operating systems.	**N/A**
220.2b	Ionizing Radiation. The payload shall include the radiation protection features/mass shielding required to insure that the crewmember dose rates from naturally occurring space radiation are kept as low as reasonably achievable (ALARA). Exposure levels shall not exceed the limits define din Figure 5.7.2.2.1-2 of NASA-STD-3000.	**N/A**
220.2c	Mechanical Hazards. Payload and equipment design shall protect crewmembers from sharp edges, protrusions, etc., during all crew operations. Translation paths and adjacent equipment shall be designed to minimize the possibility of entanglement or injury to crewmembers.	**N/A**
220.2d	Thermal Hazards. During normal operations, crewmembers shall not be exposed to high or low surface temperature extremes. Protection shall be provided against continuous skin contact with surfaces above 45 degrees Centigrade (113 degrees Fahrenheit) or below 4 degrees Centigrade (39 degrees Fahrenheit). Safeguards such as warning labels, protective devices or special design features to protect the crew from surface temperatures outside these safe limits, shall be provided for both nominal and contingency operations.	**N/A**
220.2e	Electrical Hazards. Grounding, bonding, and insulation shall be provided for all electrical equipment to protect the crew from electric shock during nominal and contingency operational phases while the crew is in the payload.	**N/A**

220.2f	Lighting. The lighting illumination level provided throughout the payload shall permit planned crew activities without injury. A backup-secondary lighting system shall be provided consistent with emergency egress requirements or in case of failure of the primary lighting system.	**N/A**
220.3	Fire Protection A fire protection system comprised of fire detection, warning, and Halon 1301 or equivalent suppression devices shall be provided in the payload . The fire protection system shall encompass both hardware and crew procedures for adequate control of the fire hazard within the cabin volume as well as within equipment racks within the pressurized hull. The fire protection system shall incorporate test and checkout capabilities such that the operational readiness of the entire system can be verified by the crewmembers. The fire protection system shall have redundant electrical power sources and shall incorporate redundant detection and warning capability and redundant activation of suppressant devices. Fire detection annunciation and control of the payload fire protection system shall be provided to the crew in both the Orbiter and payload during all Orbiter/payload attached mission phases.	**N/A**
220.4	Emergency Safing	**N/A**
220.4a	Crew Egress. The payload design shall be compatible with emergency safing and rapid crew escape. Crewmembers shall be provided with clearly defined escape routes for emergency egress in the event of a hazardous condition. Where practical, dual escape routes from all activity areas shall be provided. Payload equipment location shall provide for protection of compartment entry/exit paths in the event of an accident. Routing of hardlines, cables, or hoses through a tunnel or hatch which could hinder crew escape or interfere with hatch operation for emergency egress is not permitted. Payload hatches which could impede crew escape must remain open during all crew operations.	**N/A**

220.4b	Electrical System. The payload electrical power distribution system shall have the capability to remove all electrical power from the payload including termination of power from both the payload and Orbiter sources. This capability shall be available to the crew in both the payload and the Orbiter. Separate safing systems, however, shall be used for nominal payload functions and for essential/emergency functions (e.g., the fire protection, caution and warning, and emergency lighting, etc.). Essential/emergency functions shall be powered from a dedicated electrical power bus with redundant power sources.	**N/A**
220.5	Hatches A hatch shall be provided to isolate the payload from the Orbiter cabin. Payload latch design shall be compatible with emergency crew egress. Payloads shall provide a capability to allow a visual inspection of the interior of the payload prior to hatch opening and crew ingress. All operable hatches that could close and latch inadvertently, thereby blocking an escape route, shall have a redundant (backup) opening mechanism and shall be capable of being operated from both sides. External pressure hatches shall be self-sealing. Hatches shall have a pressure difference indicator clearly visible to the crewmember operating the hatch and a pressure equalization device. All hatches shall nominally be operable without detachable tools or operating devices and shall be designed to prevent inadvertent opening prior to complete pressure equalization. The payload/Orbiter interface shall provide or Orbiter crew EVA access to the payload bay while the payload is attached to the Orbiter.	**N/A**
220.6	Caution and Warning The payload shall incorporate a caution and warning system. All crew safety caution and warning parameters shall be redundantly monitored and shall cause annunciation in both the Orbiter and payload. As a minimum, payload total pressure, cabin fan differential pressure, fire detection, oxygen partial pressure and carbon dioxide partial pressure shall be monitored. The status of all monitored parameters shall be available to the crew in the Orbiter prior to entry into the payload. The caution and warning system shall include test provisions to allow the payload crewmembers to verify proper operation of the system. The payload provided alert system shall be consistent with Orbiter annunciation practices.	**N/A**
220.7	Windows	**N/A**

220.7a	Structural Design. Windows shall be provided in the payload only when necessary for essential mission operation, and all assemblies shall provide a redundant pressure pane. The pressure panes shall be protected from damage by external impact. The structural design of window panes in the pressure hull shall provide a minimum initial ultimate factor of safety of 3.0 and an end-of-life minimum factor of safety of 1.4. Window design shall be based on fracture mechanics considering flaw growth over the design life of the payload.	**N/A**
220.7b	Transmissivity. The transmissivity of payload windows shall be based on protection of the crew from exposure to excess levels of naturally occurring nonionizing radiation. Exposure of the skin and eyes of crewmembers to nonionizing radiation shall not exceed the threshold limit values (TLV's) set and proposed by the American Conference of Governmental Industrial Hygienists (ACGIH) as specified in "Threshold Limit Values and Biological Exposure Indices for 1987-1988"or its subsequent revisions. Window design shall be coordinated with other shielding protection design to comply with the ionizing radiation limits specified in paragraph 220.2b.	**N/A**
220.8	Communications Voice communications, compatible with the Orbiter communications system, shall be provided between the Orbiter crew and payload crewmembers during all manned operations.	**N/A**
220.9	Pressure Hull The design of the manned pressure compartment shall comply with the structural design requirements of paragraphs 208.1 and 208.2. The hull maximum design pressure (MDP) shall be determined as defined in paragraph 208.4. The ultimate factor of safety of hull design shall be equal to or greater than 2.0 for both the MDP and the maximum negative pressure differential the hull may be subjected to during normal and contingency operations or as the result of two credible failures. The pressure hull shall be designed to leak-before-burst criteria. Structural verification shall be in accordance with NSTS 14046.	**SSP 30559, Structural Design and Verification Requirements** **3.3.1 SHUTTLE TRANSPORT TO/FROM ORBIT** All Space Station flight hardware structure shall be designed to the factors of safety (FS) specified in Table 3.3.1-1, Factors of Safety for Test Verified Structure, or as modified by the factors specified in paragraphs 3.0 and 4.0 of this document.

Traceability of NSTS 18798A Interpretation Letters to ISS safety requirements

NSTS 18798A Interpretation Letter number	**Title**	**Target Spec./para. number**
TA-87-079	Mandatory Requirement Changes for Payloads Using NHB 1700.7A	Not Required
ES52-87-238M	Pressure Vessel Safety in Abort Condition	Relief to existing requirement
NS2/89-M031	Orbiter Failure Modes with Payload Impact	4.3.6.13.2
PH-M139-80	Payload Power Feeder Reliability	4.3.6.13.2
TA-88-018	Monitoring for Safety	
NS2/82-L095	Rotation of a Payload S&A Device	No SRM in program
TA-89-009	Safe Distance for Operation of Liquid Propellant Thrusters	Covered in NSTS 1700.7B, Will only be applicable to Russian Segment
NS2/87-L051	Pyrotechnically operated isolation valves	Will only be applicable to Russian Segment
NS2/85-L274	Latch valve overheating in Hydrazine systems	Will only be applicable to Russian Segment
NS2/863-L069	Catalytic effect of materials on hydrazine decomposition	Will only be applicable to Russian Segment
NS2/86-L206	Temperature limits in Bipropellant systems	Will only be applicable to Russian Segment
NS2/85-L187	Cargo produced radiation from transmitting antenna systems	**End Item Boilerplate** **3.3.6.13.7 Allowable RF radiation levels** <End Item> transmiters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.
TJ2-87-136	Effects of Orbiter Ku-Band Radiation	Information only

TA-88-025	Rapid Safing	**End Item Boilerplate** **3.3.6.13.5 Contingency Return and Rapid Safing.** The <End Item> shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop. For emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes. For a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements apply to <End Item> hardware with direct interfaces with the Orbiter: **3.3.6.13.5.1 Emergency deorbit** The <End Item> hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-<End Item> hardware operations. **3.3.6.13.5.2 Next primary landing site contingency deorbit** The <End Item> hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency deorbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-<End Item> hardware operations. (Need to add the details from the interpretation letter)
ES52-89-015L	Fracture Control for Payloads	Not required
ES52-88-200L	Fracture Control ductile screening and visual inspection	Not required
ES2-47-87	Certification Requirements for Beryllium	**NSTS 14046B**
TA-88-074	Special certification of burst disk	**SSP 30559, Structural Design and Verification Requirements** **3.1.9 PRESSURIZED STORAGE CONTAINERS** Storage containers which are classified as pressure vessels shall meet the following requirements: - Pressure vessels shall be designed and fabricated under an approved fracture control program and be in accordance with requirements specified in SSP 30558, Fracture Control Requirements for Space Station. - The storage containers shall be protected from over-pressure if attached to a system with higher pressure. The maximum operating pressure of pressure-fed storage containers shall accommodate any two system failures such as regulators, relief devices, etc.

EP5-88-L278	Standards for pyrotechnic on NSTS Payloads	**End Item Boilerplate** **3.3.6.5 Pyrotechnics.** **3.3.6.5.1 Pyrotechnics for USOS application.** **3.3.6.5.1.1 NASA Standard Initiators** NASA Standard Initiators (NSI's) shall be used for all safety critical pyrotechnic functions. **3.3.6.5.1.2 Firing circuit design** Firing circuit design shall be in accordance with the requirements for MIL-STD-1576 except paragraph 5.12.3.1.e, unconnected (unpowered) launch elements may use resistors with values less than 100 ohms or relay contacts to short the NSI leads. **3.3.6.5.1.3 Pyrotechnic operated devices** Pyrotechnic operated devices shall be designed and tested to the requirements of NSTS 08060.
NS2/85-L303	Shielding payload pyrotechnic devices	**End Item Boilerplate** **3.3.6.5 Pyrotechnics.**
ER-87-326	Payload wire sizing and circuit protection	**End Item Boilerplate** **3.3.6.8.1 Electrical power circuit overloads.** **3.3.6.8.1.1 Circuit overload protection** Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits. **3.3.6.8.1.2 Protective device sizing** Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded. **3.3.6.8.1.3 Bent pin or conductive contamination** **a.** <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function. **b.** Conductive contamination as a similar cause shall be precluded.

NS2/81-M082	Ignition of flammable payload bay atmosphere	**End Item Boilerplate** **3.3.6.13.6 Flammable Atmosphere.** **3.3.6.13.6.1 Normal functions** During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) <End Item> functions shall not cause ignition of a potential flammable payload bay atmosphere. **3.3.6.13.6.2 Electrical ignition sources** Electrical ignition sources shall not be exposed. **3.3.6.13.6.3 Surface temperatures** Surface temperatures shall be below 352 degrees F. **3.3.6.13.6.4 Conductive surfaces** Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1. 4.3.6.13.6 Include (a) and (b) from letter.
ES2-89-10	Protecting windows from damage	**SSP 30560, Glass, Window, and Ceramic Structural Design and Verification Requirements**
TA-89-064	Pressurized Stabilized Tanks	**SSP 30559, Structural Design and Verification Requirements** **3.1.9 PRESSURIZED STORAGE CONTAINERS** Storage containers which are classified as pressure vessels shall meet the following requirements: - Pressure vessels shall be designed and fabricated under an approved fracture control program and be in accordance with requirements specified in SSP 30558, Fracture Control Requirements for Space Station. - The storage containers shall be protected from over-pressure if attached to a system with higher pressure. The maximum operating pressure of pressure-fed storage containers shall accommodate any two system failures such as regulators, relief devices, etc.
DH-89-149	Payload Malfunction Procedures	

TA-90-008	Pressure Vessel Safety in Abort Condition	**SSP 30559, Structural Design and Verification Requirements** **3.1.9 PRESSURIZED STORAGE CONTAINERS** Storage containers which are classified as pressure vessels shall meet the following requirements: - Pressure vessels shall be designed and fabricated under an approved fracture control program and be in accordance with requirements specified in SSP 30558, Fracture Control Requirements for Space Station. - The storage containers shall be protected from over-pressure if attached to a system with higher pressure. The maximum operating pressure of pressure-fed storage containers shall accommodate any two system failures such as regulators, relief devices, etc.
TA-89-085	SPACELAB Module Rapid Safing	
ET12-90-115	Separation of Redundant Safety Critical Circuits	
TA-91-006	Cargo Bay Power Feeder Fault Tolerance	
NS2/90-208	Structural Requirements for contingency deorbit	**SSP 30559, Structural Design and Verification Requirements** **3.2.1 SHUTTLE PAYLOAD CONFIGURATION DESIGN LOADS** For lift-off, ascent, on orbit, descent, and landing using Shuttle, Space Station structure shall be designed to maintain required functionality and positive margins when subjected to all static and dynamic loads and thermal environments as defined in NSTS 07700, Volume XIV, Space Shuttle System Payload Accommodations, and ICD 2-19001, Shuttle Orbiter/Cargo Standard Interfaces.
TA-91-062	Payload Commanding	
TA-91-077	Circuit Design for payloads using energy storage devices for pyrotechnic firing circuits	Information only

TA-92-013	Low Risk Fracture Parts	**SSP 30558, Fracture Control Requirements for Space Station** **4.2.4.1 Remote Possibility of Significant Crack Like Defects** Assurance against the presence of a significant crack-like defect shall ve achieved by compliance with the following criteria: a. The part shall be fabricated from a well-characterized metal which is not sensitive to stress corrosion cracking as defined in MSFC-SPEC-522B, or MSFC-HDBK-527/JSC 09604. If other than Table I or A-rated materials as classified respectively in these documents must be used, suitability for the specific application shall be documented by a Materials Usage Agreement (MUA). MUA forms contained in the cited documents, or equivalent, shall be used.
TA-92-049	Pyrotechnically operated isolation valves	May apply to the international partners
TA-92-038	Protection of payload electrical power circuits	**End Item Boilerplate** **3.3.6.8.1 Electrical power circuit overloads.** **3.3.6.8.1.1 Circuit overload protection** Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits. **3.3.6.8.1.2 Protective device sizing** Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded. **3.3.6.8.1.3 Bent pin or conductive contamination** **a.** <End Item> electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function. **b.** Conductive contamination as a similar cause shall be precluded.
TC3-93-016	Payloads Use of Orbiter General Purpose Computer	
TA-93-037	Structural Integrity following Mechanism Failures	**SSP 30558, Fracture Control Requirements for Space Station** **4.1.3**

APPENDIX D-Attached Pressurized Module Segment Specification

3.3.6 Safety.

3.3.6.1 General.

3.3.6.1.1 Catastrophic Hazards.

Catastrophic hazards shall be controlled such that no combination of two failures, or two operator errors (See 6.1), or one of each can result in a catastrophic hazards event. Compliance with this requirement may be accomplished at the APM level or through a combination of hazard controls (See 6.1) at the Segment/ISS levels.

3.3.6.1.2 Critical Hazards.

Critical hazards shall be controlled such that no single failure or single operator error can result in a critical hazardous event. Compliance with this requirement may be accomplished at the APM level or through a combination of hazard controls at the Segment/ISS levels.

3.3.6.1.3 Design for minimum risk.

Hazards related to ”Design for Minimum Risk” (See 6.1) areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of ”Design for Minimum Risk” areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards.

3.3.6.1.4.1 Inadvertent operation resulting in critical hazards.

A function whose inadvertent operation could result in a critical hazard (See 6.1) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the APM level or through a combination of hazard controls at the Segment/ISS levels.

3.3.6.1.4.2 Loss of function resulting in critical hazards.

Where loss of a function could result in a critical hazard, no single credible failure (See 6.1) shall cause loss of that function and the function shall be monitored and controlled Where operator input to control the hazard would be untimely or ineffective, the APM shall have the capability to automatically safe the function prior to the time to critical hazardous effect. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards.

3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See 6.1), whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

Note: Compliance with this requirement may be accomplished at the APM level or through a combination of hazard controls (see 6.1) at the Segment/ISS levels.

3.3.6.1.5.2 Loss of function resulting in catastrophic hazards.

Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.
b. The function shall be monitored such that necessary safety data that require operator or automated action for safing is acquired prior to the time to catastrophic hazardous effects. Where operator input to control the hazard would be untimely or ineffective, the APM shall have the capability to automatically safe the function prior to the time to catastrophic hazardous effect.

3.3.6.1.6 Subsequent induced loads.

If a component of the APM is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure

tolerant design provisions to safe the component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard

3.3.6.1.7 Safety interlocks.

Safety interlocks (See 6.1) shall be provided to prevent unsafe operations

3.3.6.1.8 Environmental compatibility.

APM functions shall be safe (See 6.1) in the applicable worst case natural and induced environments defined in paragraph 3.2.5, ”Environmental Conditions” or as defined in a payload integration plan, mission integration plan and/or interface control document.

3.3.6.2 Hazard Detection and Safing.

3.3.6.2.1 Reserved.

3.3.6.2.2 Monitors.

3.3.6.2.2.1 Status information.

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention.

Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function.

3.3.6.2.2.3 Loss of input or failure.

Loss of input or failure of the monitor shall be identifiable.

3.3.6.2.2.4 Launch site availability.

Reserved

3.3.6.2.2.5 Flight crew availability.

Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

3.3.6.2.3 Near-real time monitoring.

Near-real time monitoring (See 6.1) of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, such that necessary safety data that require operator or automated action for safing is acquired prior to the time to hazardous effects. The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard.

3.3.6.2.4 Real Time Monitoring.

3.3.6.2.4.1 Maintain status of hazard controls.

The APM shall provide real-time monitoring (See 6.1) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the APM is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground monitoring

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within time to effect of the hazard upon loss of communications with the ground.

3.3.6.3 Command and computer control of hazardous functions.

The computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038B **(TBR)**

3.3.6.4 Hazardous Materials.

3.3.6.4.1 Hazardous fluid containment failure tolerance.

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558 (Fracture Control Requirements for Space Station) or an equivalent ESA standard (MS-ESA-RQ-008).

3.3.6.4.2 Storage of Hazardous Chemicals.

Reserved

3.3.6.5 Pyrotechnics.

Reserved

3.3.6.6 Radiation.

3.3.6.6.1 Non-ionizing Radiation.

The APM shall limit the levels of nonionizing radiation of the APM in accordance with SSP 50005, paragraphs 5.7.3.2 and 5.7.3.2.1 to provide personnel protection.

3.3.6.6.2 Transmitters
Reserved

3.3.6.7 Optics and Lasers.

3.3.6.7.1 Lasers.
Reserved

3.3.6.7.2 Optical Requirements.
Reserved

3.3.6.8 Electrical Safety.

3.3.6.8.1 Electrical power circuit overloads.

3.3.6.8.1.1 Circuit Overload Protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective Device Sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) or ESA equivalent specification (PSS-01-301) are precluded.

3.3.6.8.1.3 Bent Pin or Conductive Contamination

a. APM electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

b. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock.

a. The crew in APM shall not be exposed to un-insulated electrical power leads.

b. The crew in the APM shall be protected from electrical hazards in accordance with SSP 50005, section 6.4.3 Electrical Hazards Design Requirements

3.3.6.8.3 Re-application of power.

For the APM the crew alone shall have positive local control of reapplication of power to each enclosed power location
For the APM the crew shall be able to remove power and positively verify local power to each enclosed powered volume.

3.3.6.8.4 Batteries.

a. APM batteries which can pose a safety hazard shall be isolated and/or provided with safety venting systems and/or explosion protection.

b. In addition thermal control and charge/discharge protection for APM batteries shall be provided where applicable

3.3.6.9 Liquid Propellant Propulsion Systems

Reserved

3.3.6.10 Fire protection.

3.3.6.10.1 Manual activation.

The APM shall have the capability of crew initiated notification of a fire event within one minute after crew detection.

3.3.6.10.2 Isolation.

The APM shall ensure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.

3.3.6.10.3 Fire Suppressant Application.

The APM shall accommodate the application of CO2 fire suppressant at each enclosed location containing a potential fire source.

3.3.6.10.4. Fire Suppressant

The fire extinguishing agent shall be CO2. The release of CO2 suppressant into the isolated APM shall not raise the atmosphere CO2 concentration above 34.2 mm-Hg partial pressure.

3.3.6.10.5 Restorable Suppression.

Fixed fire suppression, where installed, shall be restorable after discharge.
Fixed Fire suppression, where installed, shall incorporate a disabling feature to prevent inadvertent activation during its maintenance.

3.3.6.10.6 Power Removal

Fixed fire suppression, where installed, shall remain functional after the removal of power to a location after detection of a fire event.

3.3.6.10.7 Confirmation

The APM shall confirm a fire event condition prior to any automated isolation, or suppression. Confirmation consists of at least two validated indications of fire/smoke from a detector.

3.3.6.10.8 Verification of Suppressant

On-board verification of suppressant availability shall be provided.

3.3.6.10.9 PBA and PFE locations

One PBA and one PFE shall be located in pressurized elements less than or equal to 24 feet in accessible interior length. Where the element exceeds 24 feet in accessible interior length, a PBA/PE set shall be located within 12 feet of each end of the element. At least one PBA shall be located within 3 feet of each PFE.

3.3.6.10.10 Loss of detection.

Reserved

3.3.6.10.11 Manual alarm activation

Reserved

3.3.6.11 Constraints.

3.3.6.11.1 Reserved.

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance.

3.3.6.11.2.1 Pressure differential tolerance.

APM equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard .

3.3.6.11.2.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards.

3.3.6.11.3. Emergency IVA egress.

The time required to accomplish safe emergency IVA egress from the APM shall not exceed 3 minutes, including the time required to secure the node hatch.

3.3.6.11.4.

Reserved.

3.3.6.11.5

Reserved.

3.3.6.11.6 Component hazardous energy provision.

Components, which retain hazardous energy potential shall either be designed to prevent a crewmember conducting maintenance from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful

3.3.6.11.7 Hatch opening.

The APM shall provide the capability to control pressure differential and verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels of selected compounds from Table 1 and provide visual inspection of the interior of the pressurized volume prior to crew ingress.

TABLE 1. Spacecraft maximum allowable concentrations						
		Potential Exposure Period				
Chemical		1 h	24 h	7 d	30 d	180 d
Acetaldehyde	mg/m^3	20	10	4	4	4
Acrolein	mg/m^3	0.2	0.08	0.03	0.03	0.03
Ammonia	mg/m^3	20	14	7	7	7
Carbon Dioxide	mm Hg	10	10	5.3	5.3	5.3
Carbon monoxide	mg/m^3	60	20	10	10	10
1,2-Dichloroethane	mg/m^3	2	2	2	2	1
2-Ethoxyethanol	mg/m^3	40	40	3	2	0.3
Formaldehyde	mg/m^3	0.5	0.12	0.05	0.05	0.05
Freon 113	mg/m^3	400	400	400	400	400
Hydrazine	mg/m^3	5	0.4	0.05	0.03	0.005
Hydrogen	mg/m^3	340	340	340	340	340
Indole	mg/m^3	5	1.5	0.25	0.25	0.25
Mercury	mg/m^3	0.1	0.02	0.01	0.01	0.01
Methane	mg/m^3	3800	3800	3800	3800	3800
Methanol	mg/m^3	40	13	9	9	9
Methyl ethyl ketone	mg/m^3	150	150	30	30	30
Methyl hydrazine	mg/m^3	0.004	0.004	0.004	0.004	0.004
Dichloromethane	mg/m^3	350	120	50	20	10
Octamethyltrisiloxane	mg/m^3	4000	2000	1000	200	40
2-Propanol	mg/m^3	1000	240	150	150	150
Toluene	mg/m^3	60	60	60	60	60
Trichloroethylene	mg/m^3	270	60	50	20	10
Trimethysilanol	mg/m^3	600	70	40	40	40
Xylene	mg/m^3	430	430	220	220	220

3.3.6.11.8 Reserved.

3.3.6.11.9 Reserved.

3.3.6.11.10 Reserved.

3.3.6.11.11 Reserved.

3.3.6.11.12 Hazardous Gas Accumulation.

3.3.6.11.12.1 Accumulation prevention.

The APM shall provide the capability to prevent uncontrolled hazardous accumulations of gases.

3.3.6.11.12.2 Detection, monitoring, and control

Detection, monitoring, and control of hazardous gases or vapors shall be required in critical areas and closed compartments. Detection and monitoring will be provided at the system level.

3.3.6.11.13 Equipment clearance for entrapment hazard.

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Light Fixture.

Light fixtures assemblies shall incorporate features to contain all glass fragments in the case of lamp breakage.

3.3.6.12 Human engineering safety.

3.3.6.12.1 Internal volume touch temperature.

3.3.6.12.1.1 Exposed Surfaces temperatures.

Exposed surfaces within pressurized elements shall not exceed a high temperature of 45 degrees centigrade (113 degrees Fahrenheit) and a low temperature less than 4 degrees centigrade (40 degrees Fahrenheit).

3.3.6.12.2 External touch temperature

The suit shall be protected from high or low touch temperature extremes for the following:

3.3.6.12.2.1 Incidental contact.For incidental contact

APM external temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates specified in Table XVII, SSP 41000B Heat Transfer rates, to protect EVA suited crew members.

TABLE 2. Heat transfer rates

Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate(1) (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52(2)
	Incidental (0.5 max)	113	1.444	176.2(3)
Cold Object	Unlimited	40	1.062	-132.7(2)
	Incidental (0.5 max)	40	1.478	-325.2(3)

Notes:
1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

3.3.6.12.2.2 Unlimited contact

For unlimited contact, APM external temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table XVIII SSP 41000B, Designated EVA Interfaces, limit heat transfer rates as specified in Table XVII, SSP 41000B Heat Transfer Rates, to protect EVA suited crew members.

TABLE 3. Designated EVA interfaces
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection.

3.3.6.12.3.1 Sharp edges

APM equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb.

3.3.6.12.3.2 Thin materials

Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches.

3.3.6.12.3.3 Planned maintenance or storage

Equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.1

3.3.6.12.4 Internal corner and edge protection.

3.3.6.12.4.1 Equipment exposed to crew activity

Surfaces of APM equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge

requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 Equipment exposed only during planned maintenance activities

Corners and edges of material, equipment or ORUs which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

3.3.6.12.5 Contingency repressurization.

Controls necessary for restoring a depressurized module to normal operating pressurized conditions shall be capable of being manually operated by an EVA suited crewperson as specified in SSP 50005, paragraph 14.3.

3.3.6.12.6 Latches.

Latches or similar devices shall be designed to prevent entrapment of crew member appendages.

3.3.6.12.7 Screws and bolts.

Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 Safety Critical Fasteners.

Safety critical fasteners shall be designed to prevent inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls.

Levers, cranks, hooks and controls shall be located or otherwise suitably protected such that they cannot pinch, snag, cut, or abrade the crew members or their clothing.

3.3.6.12.10 Burrs.

Exposed surfaces shall be free of burrs.

3.3.6.12.11 Holes

3.3.6.12.11.1 Equipment located inside habitable volumes.

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes.

3.3.6.12.11.2 Equipment located outside habitable volumes.

Holes (round, slotted, polygonal) in EVA translation hand rails/holds shall be 1.0 inches or greater in diameter.

3.3.6.12.12 Protrusions

.Equipment except for translation aids identified in Table 3 (Designated EVA Interfaces) shall not protrude into the 50 inch horizontal by 72 inch vertical envelope of the CETA/MT corridor, or the 43 inch horizontal envelope of the primary and secondary translation path.

3.3.6.12.13 Pinch points.

Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crew member appendages.

3.3.6.12.14 Emergency Ingress

The APM shall design EVA translation paths and aids such that an EVA crewmember can complete an emergency ingress within 30 minutes into a pressurized volume from EVA worksites on APM hardware.

3.3.6.12.15 **Reserved.**

3.3.6.12.16 Flexhoses.

Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware.

3.3.6.12.17 Translation routes and established worksites.

For protection from hazards along translation routes and established worksites the following apply:

3.3.6.12.17.1 Primary translation routes and established worksites

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.

b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.17.2 Secondary translation routes and established worksites

External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded and controlled as specified in Table 4.

TABLE 4. Control for exposed risks to EVA crew

Risk Type	Hazard	Control Method *
Innate Characteristics	Non-Ionizing Radiation (Antennas transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards
	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Connectors	Warning Strips and Placards
	Thermal (>235 degrees F or < -180 degrees F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards
	Narrow Passageways Protrusions	Placards
	Structure Sensitive to EVA Loads	Placards
	Pinch Points	Placards

	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards
CETA Corridor	Structural Impacts - Mobile Transporter - End of Rail	Color-coded Anodized yellow with black cross-hatching
Note: * Control methods shall be designed in accordance with SSP 50006.		

3.3.6.12.17.3 EVA crewmember contact isolation

APM hardware which cannot be controlled by design features to comply with ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crewmember contact.

3.3.6.12.18 Moving or rotating equipment.

For EVA, where the EVA crewmwmber is in the vicinity of moving or rotating equipment, the EVA crewmember shall be protected from that equipment.

3.3.6.13 Launch vehicle interfaces and services.

The following requirements in section 3.3.6.13 apply only to hardware that will be launched on the Space Shuttle.

3.3.6.13.1 Safe Without Space Shuttle Program Services.

If the APM receives safety critical services from the Space Shuttle, the APM shall maintain the Following capabilities:

3.3.6.13.1.1 Fault tolerance/safety margins.

The APM shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions.

During Orbiter emergency conditions, the APM shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter Services.

When Orbiter services are to be utilized to control APM hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions.

Inadvertent deployment, separation or jettison of the APM hardware or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4, 3.3.6.1.5 and 3.3.6.2.2 , 3.3.6.2.3, and 3.3.6.2.4 apply.

3.3.6.13.4 Planned Deployment/Extension Functions.

3.3.6.13.4.1 Violation of Orbiter payload door envelope.

If a component of the APM or any APM orbital support equipment (OSE) violates the payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance.

The combination of these primary and backup methods shall be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency Return and Rapid Safing.

The APM shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and de-orbit when emergency conditions develop. For emergency de-orbit, the payload bay doors can be closed within 20 minutes with the de-orbit burn in 30 minutes. For a next primary landing site contingency de-orbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and de-orbit burn would occur 2 hours and 40 minutes later. The following requirements apply to APM hardware with direct interfaces with the Orbiter:

3.3.6.13.5.1 Emergency de-orbit.

The APM hardware shall have at least one system to allow the Orbiter to meet the emergency de-orbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-APM hardware operations.

3.3.6.13.5.2 Next primary landing site contingency de-orbit.

The APM hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency de-orbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-APM hardware operations.

3.3.6.13.6 Flammable Atmosphere.

3.3.6.13.6.1 Normal functions

During Orbiter entry, landing, and post-landing operations (whether planned or contingency), the normal (no failures) APM functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical ignition sources.

Electrical ignition sources shall not be exposed.

3.3.6.13.6.3 Surface temperatures.

Surface temperatures shall be below 352 degrees F.

3.3.6.13.6.4 Conductive surfaces.

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1.

3.3.6.13.7 Allowable RF radiation levels.

APM transmitters located in or out of the Orbiter payload bay which has the capability to emit radiation levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachment 1 (ICD 2-19001) shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when

there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed the NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001) limits by more that 6 decibels(dB) in which case two of three inhibits must be monitored.

3.3.6.13.8 Lightning protection.

APM electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard.

3.3.6.13.9 Orbiter vent/dump provisions.

3.3.6.13.9.1 Release or ejection of hazardous material.

APM hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS.

3.3.6.13.9.2 Fluid system containment.

APM shall be designed to contain both hazardous and non-hazardous fluids when in the presence of the Orbiter.

3.3.6.13.10 Sealed Compartments.

APM components, located in regions of the Orbiter other than the habitable volume, shall be designed to withstand the decompression and repressurization environments associated with ascent or descent without resulting in a hazard.

3.3.6.14 Ground Support equipment Safety Requirements for Space Shuttle launch of APM hardware.

The APM ground support equipment designated to be processed at the Space Shuttle site shall be in accordance with SSP 50004 and KHB 1700.7.

Safety Definitions

Catastrophic Hazard -
Any hazard which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the Orbiter or ISS. Note: For safety failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with the ISS launch elements.

Credible failure -
A condition that has a potential of occurring based on actual failure modes in similar systems.

Critical Hazard -
Any hazard which may cause a non-disabling personnel injury, severe occupational illness; loss of a major ISS element; or involves damage to the Orbiter or a ground facility. Note: For safety failure tolerance considerations, critical hazards include the loss of ISS elements that are not in the critical path for station survival or which can be restored through contingency repair.

Design for Minimum Risk -
Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance. criteria. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance must be imposed upon external system that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure of the pressure vessel. Examples are mechanisms, structures, glass, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Fire Event -
Localized or propagating combustion, pyrolysis, smoldering, or other thermal degradation process characterized by the potentially hazardous release of energy, particulates, or gases

Fire Protection (FP) Location -
Any partitioned volume of a pressurized element.FP locations may be enclosed or open.

Flight Crew Support Equipment -

This is limited to the shower location, the exercise location and commode/urinal location.

Hazard -
The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Independent Inhibit -
Two or more inhibits are independent if no single failure, event or environment can eliminate more than one inhibit.

Independent Safing Action -
An independent safing action is an action generated by a non failed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent safing actions from transitioning the system to a safe state

Inhibit -
A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.).

Local control -
A capability to accomplish a function at the direction of the crew within the applicable on-orbit module and also prevent reconfiguration of the function by an external entity during the specified period.

Near Real Time Monitoring -
Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). Note: The capability of the hardware and software to provide the updated data for near real-time monitoring data is generally the lowest available frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Operator Error -
An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. Note: The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or wrong keystroke or an inadvertent switch throw.

Potential Fire Source -

Any electrical, chemical, or other energy source capable of creating a fire event (e.g. electrically powered equipment).

Rapid Safing -
The capability of the Orbiter to accomplish an emergency de-orbit or a de-orbit contingency to the next primary landing site.

Real Time Monitoring -
Notification of changes in inhibit or safety status to the crew at a rate adequate to allow for appropriate reaction to a change in the status. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user to react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Safe -
A general term denoting relative freedom from and low probability of: personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss excessive degradation of the function of critical equipment.

Safing -
An action or sequence of actions necessary to place systems, subsystems or component parts into predetermined safe conditions.

Safety Critical function -
Function that if lost or degraded or which through inadvertent operation would result in a catastrophic or critical consequence.

APPENDIX E - JEM SEGMENT SPECIFICATION

3.3.6 Safety.

3.3.6.1 General

3.3.6.1.1 Catastrophic Hazards

The JEM shall be designed such that no combination of two failures, or two operator errors , or one of each can result in a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or a major ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.2 Critical Hazards.

The JEM shall be designed such that no single failure or single operator error can result in a nondisabling personnel injury, severe occupational illness; loss of a major ISS element on-orbit life sustaining function or emergency system, or involves damage to the Orbiter or a ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.3 Design for minimum risk.

Hazards related to ”Design for Minimum Risk” areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of ”Design for Minimum Risk” areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards.

3.3.6.1.4.1 Inadvertent operation resulting in critical hazards.

A function whose inadvertent operation could result in a critical hazard shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of function resulting in critical hazards.

Where loss of a function could result in a critical hazard, no single credible failure shall cause loss of that function and the function shall be monitored and controlled in accordance with the ISS capabilities ”Monitor System Status” and Respond to Loss of Function”. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards.

3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards

Compliance with requirements a, b and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits , whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in catastrophic hazards

Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

b. The function shall be monitored and controlled in accordance with the ISS capabilities ”Monitor System Status” and ”Respond to Loss of Function”..

3.3.6.1.6 Subsequent induced loads

If a component of the JEM is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the component appropriate to the hazard level. Safing

may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard.

3.3.6.1.7 Safety interlocks.

Safety interlocks/inhibits or safety devices shall be provided to prevent unsafe operations when access to JEM equipment is required for maintenance.

3.3.6.1.8 Environmental compatibility.

JEM functions shall be safe in the applicable worst case natural and induced environments defined in paragraph 3.2.6, "Environmental Conditions" or as defined in a payload integration plan , mission integration plan and/or interface control document.

3.3.6.2 Hazard Detection and Safing

3.3.6.2.1 Reserved.

3.3.6.2.2 Monitors.

3.3.6.2.2.1 Status information

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention

Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function.

3.3.6.2.2.3 Loss of input or failure

Loss of input or failure of the monitor shall be identifiable.

3.3.6.2.2.4 Launch site availability

Monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 Flight crew availability

Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

3.3.6.2.3 Near-real time monitoring.

Near-real time monitoring of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, "Respond to Loss of Function". The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard.

3.3.6.2.4 Real Time Monitoring.

3.3.6.2.4.1 Maintain status of hazard controls

The JEM shall provide real-time monitoring) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the JEM is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground monitoring

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within time to effect of the hazard upon loss of communications with the ground.

3.3.6.3 Command and computer control of hazardous functions

3.3.6.3.1 Computer control of hazardous functions

The computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038B **(TBR).**

3.3.6.4 Hazardous Materials

3.3.6.4.1 Hazardous fluid containment failure tolerance.

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558.

3.3.6.4.2 Storage of Hazardous Chemicals.

Hazardous experiment payload chemicals/materials shall be stored only in International Standard Payload Racks (ISPRs) located in U.S. Laboratory or Logistics Modules.

3.3.6.5 Pyrotechnics. - Reserved

3.3.6.6 Radiation

3.3.6.6.1 Nonionizing Radiation.

The JEM shall limit the levels of nonionizing radiation of the JEM in accordance with SSP 50005, paragraphs 5.7.3.2 and 5.7.3.2.1 to provide personnel protection.

3.3.6.6.2 JEM Transmitters.

JEM Transmitters shall not irradiate the Orbiter at levels exceeding the allowable limits as specified in NSTS 07700, Volume XIV, Attachments 1 (ICD 2-19001). A two fault tolerant combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation of the Orbiter. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed Orbiter limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

3.3.6.7 Optics and Lasers.

3.3.6.7.1 Lasers - Reserved

3.3.6.7.2 Optical Requirements.

3.3.6.7.2.1 Optical instruments

Optical instruments shall prevent harmful light intensities and wavelengths from being viewed by operating personnel.

3.3.6.7.2.2 Personnel protection

Quartz windows, apertures, or beam stops and enclosures shall be used for hazardous wavelengths and intensities unless suitable protective measures are taken to protect personnel form Ultraviolet or Infrared burns or X-Ray radiation.

3.3.6.7.2.3 Direct viewing optical systems

Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be limited to levels below the maximum permissible exposure (MPE).

3.3.6.8 Electrical Safety

3.3.6.8.1 Electrical power circuit overloads.

3.3.6.8.1.1 Circuit overload protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination

a. JEM electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

b. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock.

The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3.

3.3.6.8.3 Reapplication of power.

The JEM shall provide local control of interruption and reapplication of power to each IVA maintenance area.

3.3.6.8.4 Batteries. - Reserved

3.3.6.9 Cryogenics. Reserved

3.3.6.10 Fire protection

3.3.6.10.1 Manual activation.

The JEM shall have the capability for entry of crew initiated notification of a fire event within one minute after crew detection.

3.3.6.10.2 Isolation.

The JEM shall ensure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.

3.3.6.10.3 Fire suppressant

The release of CO2 suppressant into the isolated JEM shall not raise the atmosphere CO2 concentrations above 34.2 mm-Hg partial pressure.

3.3.6.10.4 Fire suppressant application.

The JEM shall accommodate the application of carbon dioxide fire suppressant at each enclosed location containing a potential fire source.

3.3.6.10.5 PBA and PFE locations.

One (1) PBA and one (1) PFE shall be located in elements less than or equal to 24 feet in accessible interior length. Where the element exceeds 24 feet in accessible interior length, a set of PBAs and PFEs shall be located within 12 feet of each end of the element. At least one (1) PBA shall be located within three (3) feet of each PFE.

3.3.6.10.6 Fixed Suppression

Fixed fire suppression, where installed, shall incorporate a disabling feature to prevent inadvertent activation during maintenance.

3.3.6.10.7 Restorable suppression.

Fixed fire suppression, where installed, shall be restorable after discharge.

3.3.6.10.8 Power removal

Fixed fire suppression, where installed, shall remain functional after the removal of power to a location after detection of a fire event.

3.3.6.10.9 Confirmation

The JEM shall confirm a fire event condition prior to any automated isolation, or suppression. Confirmation consists of a least two validated indications of fire/smoke from a detector.

3.3.6.10.10 Verification of a suppressant

On-board verification of suppressant availability shall be provided.

3.3.6.11 Constraints

3.3.6.11.1 Reserved

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance.

3.3.6.11.2.1 Pressure differential tolerance

JEM equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard .

3.3.6.11.2.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards.

3.3.6.11.3. Emergency egress.

The JEM shall provide for safe emergency IVA egress to the remaining contiguous pressurized volumes and have the capability to isolate from other flight pressurized volumes within three minutes, including closing hatches.

3.3.6.11.4. Reserved.

3.3.6.11.5 Reserved.

3.3.6.11.6 Component hazardous energy provision.

Components, which retain hazardous energy potential shall either be designed to prevent a crewmember conducting maintenance from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful.

3.3.6.11.7 Hatch opening.

The JEM shall provide the capability to control pressure differential and verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels of selected compounds from Table 1 and provide visual inspection of the interior of the pressurized volume prior to crew ingress.

TABLE 1. Spacecraft maximum allowable concentrations						
		Potential Exposure Period				
Chemical		1 h	24 h	7 d	30 d	180 d
Acetaldehyde	mg/m^3	20	10	4	4	4
Acrolein	mg/m^3	0.2	0.08	0.03	0.03	0.03
Ammonia	mg/m^3	20	14	7	7	7
Carbon Dioxide	mm Hg	10	10	5.3	5.3	5.3
Carbon monoxide	mg/m^3	60	20	10	10	10
1,2-Dichloroethane	mg/m^3	2	2	2	2	1
2-Ethoxyethanol	mg/m^3	40	40	3	2	0.3
Formaldehyde	mg/m^3	0.5	0.12	0.05	0.05	0.05
Freon 113	mg/m^3	400	400	400	400	400
Hydrazine	mg/m^3	5	0.4	0.05	0.03	0.005
Hydrogen	mg/m^3	340	340	340	340	340
Indole	mg/m^3	5	1.5	0.25	0.25	0.25
Mercury	mg/m^3	0.1	0.02	0.01	0.01	0.01
Methane	mg/m^3	3800	3800	3800	3800	3800
Methanol	mg/m^3	40	13	9	9	9
Methyl ethyl ketone	mg/m^3	150	150	30	30	30
Methyl hydrazine	mg/m^3	0.004	0.004	0.004	0.004	0.004
Dichloromethane	mg/m^3	350	120	50	20	10
Octamethyltrisiloxane	mg/m^3	4000	2000	1000	200	40
2-Propanol	mg/m^3	1000	240	150	150	150
Toluene	mg/m^3	60	60	60	60	60
Trichloroethylene	mg/m^3	270	60	50	20	10
Trimethysilanol	mg/m^3	600	70	40	40	40
Xylene	mg/m^3	430	430	220	220	220

3.3.6.11.8 Reserved.

3.3.6.11.9 Reserved.

3.3.6.11.10 Reserved.

3.3.6.11.11 Reserved.

3.3.6.11.12 Hazardous Gas Accumulation.

3.3.6.11.12.1 Accumulation prevention

The JEM shall provide the capability to prevent uncontrolled hazardous accumulations of gases.

3.3.6.11.12.2 Detection, monitoring, and control

Reserved

3.3.6.11.13 Equipment clearance for entrapment hazard.

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Light Fixture.

Light fixtures assemblies shall incorporate features to contain all glass fragments in the case of lamp breakage.

3.3.6.11.15 Reserved.

3.3.6.12 Human engineering safety

3.3.6.12.1 Internal volume touch temperature.

The maximum allowable surface temperature for continuous contact with bare skin shall be 113 degrees Fahrenheit.

(1) Incidental or momentary bare skin contact (30 seconds or less) with surface temperatures shall not exceed 120 degrees Fahrenheit.

(2) Warning labels shall be provided to alert crewmembers to these excessive temperature levels. Guards or insulation shall be provided to prevent crewmember contact with surface temperatures in excess of 120 degrees Fahrenheit. Where contact with surfaces above this limit is required, warning labels and protective equipment shall be provided.

The minimum temperature for surfaces that must be touched with bare skin shall not be below 39 degrees Fahrenheit.

(1) Where contact with surfaces below this limit is required, warning labels and protective equipment shall be provided.

3.3.6.12.2 External touch temperature.

The suit shall be protected from high or low touch temperature extremes as follows:

3.3.6.12.2.1 Incidental contact

For incidental contact, temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates as specified in Table 2.

TABLE 2. Heat transfer rates				
Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate(1) (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52(2)
	Incidental (0.5 max)	113	1.444	176.2(3)
Cold Object	Unlimited	40	1.062	-132.7(2)
	Incidental (0.5 max)	40	1.478	-325.2(3)

Notes:
1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

3.3.6.12.2.2 Unlimited contact

For unlimited contact, temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table 3, limit heat transfer rates as specified in Table 2.

TABLE 3. Designated EVA interfaces
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection.

3.3.6.12.3.1 Sharp edges

JEM equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb.

3.3.6.12.3.2 Thin materials

Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches.

3.3.6.12.3.3 Planned maintenance or storage

Equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.1

3.3.6.12.4 Internal corner and edge protection.

3.3.6.12.4.1 Equipment exposed to crew activity

Surfaces of JEM equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 Equipment exposed only during planned maintenance activities

Corners and edges of material, equipment or ORUs which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

3.3.6.12.5 Reserved

3.3.6.12.6 Latches.

Latches or similar devices shall be designed to prevent entrapment of crewmember appendages.

3.3.6.12.7 Screws and bolts.

Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 Safety Critical Fasteners

Safety critical fasteners shall be designed to prevent inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls.

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

3.3.6.12.10 Burrs.

Exposed surfaces shall be smooth and free of burrs.

3.3.6.12.11 Holes

3.3.6.12.11.1 Equipment located inside habitable volumes

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes.

3.3.6.12.11.2 Equipment located outside habitable volumes

Holes (round, slotted, polygonal) in EVA translation hand rails/holds shall be 1.0 inches or greater in diameter.

3.3.6.12.12 Protrusions

Equipment except for translation aids identified in Table 3 shall not protrude into the 50 inch horizontal by 72 inch vertical envelope of the CETA/MT corridor, or the 43 inch horizontal envelope of the primary and secondary translation path.

3.3.6.12.13 Pinch points.

Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of

greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crewmember appendages.

3.3.6.12.14 Emergency Ingress.

The JEM shall design EVA translation paths and aids such that an EVA crewmember can complete an emergency ingress within 30 minutes into a pressurized volume from EVA worksites on JEM hardware.

3.3.6.12.15 Reserved

3.3.6.12.16 Flexhoses.

Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware.

3.3.6.12.17 Translation routes and established worksites.

For protection from hazards along translation routes and established worksites the following apply:

3.3.6.12.17.1 Primary translation routes and established worksites

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.

b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.17.2 Secondary translation routes and established worksites

External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded and controlled as specified in Table 4.

TABLE 4. Control for exposed risks to EVA crew

Risk Type	Hazard	Control Method *
Innate Characteristics	Non-Ionizing Radiation (Antennas transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards

	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Connectors	Warning Strips and Placards
	Thermal (>235 degrees F or < -180 degrees F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards
	Narrow Passageways Protrusions	Placards
	Structure Sensitive to EVA Loads	Placards
	Pinch Points	Placards
	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards
CETA Corridor	Structural Impacts - Mobile Transporter - End of Rail	Color-coded Anodized yellow with black cross-hatching
Note: * Control methods shall be designed in accordance with SSP 50006.		

3.3.6.12.17.3 EVA crewmember contact isolation

JEM hardware which cannot be controlled by design features to comply with ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crewmember contact.

3.3.6.12.18 Moving or rotating equipment.

The EVA crewmember shall be protected from moving or rotating equipment.

3.3.6.13 Launch vehicle interfaces and services.

3.3.6.13.1 Safe Without Space Shuttle Program Services.

3.3.6.13.1.1 Fault tolerance/safety margins

The JEM shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions

During Orbiter emergency conditions, JEM shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter Services.

When Orbiter services are to be utilized to control JEM hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions

Inadvertent deployment, separation or jettison of the JEM or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4, 3.3.6.1.5 and 3.3.6.2.2 apply.

3.3.6.13.4 Planned Deployment/Extension Functions - Reserved

3.3.6.13.4.1 Violation of Orbiter payload door envelope - Reserved

3.3.6.13.4.2 Method of fault tolerance Reserved

3.3.6.13.5 Contingency Return and Rapid Safing.

The JEM shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop. For emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes. For a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements apply to JEM hardware with direct interfaces with the Orbiter:

3.3.6.13.5.1 Emergency deorbit

The JEM hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-JEM hardware operations.

3.3.6.13.5.2 Next primary landing site contingency deorbit

The JEM hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency deorbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-JEM hardware operations.

3.3.6.13.6 Flammable Atmosphere.

3.3.6.13.6.1 Normal functions

During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) JEM functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical ignition sources

Electrical ignition sources shall not be exposed.

3.3.6.13.6.3 Surface temperatures

Surface temperatures shall be below 352 degrees F.

3.3.6.13.6.4 Conductive surfaces

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1.

3.3.6.13.7 Allowable RF radiation levels Reserved

3.3.6.13.8 Lightning protection

JEM electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard.

3.3.6.13.9 Orbiter vent/dump provisions

3.3.6.13.9.1 Release or ejection of hazardous material

JEM hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS.

3.3.6.13.9.2 Fluid system containment

JEM shall be designed to contain both hazardous and nonhazardous fluids when in the presence of the Orbiter.

3.3.6.13.10 Sealed Compartments.

JEM components, located in regions of the Orbiter other than the habitable volume, shall be designed to withstand the decompression and repressurization enviroments associated with ascent or descent without resulting in a hazard.

3.3.6.14 Ground interfaces and services - Space Shuttle launch

Hazards shall not be created due to the inaccessibility of flight hardware such as:.

3.3.6.14.1 Moving parts

Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.

3.3.6.14.2 Equipment requiring adjustment

Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable.

3.3.6.14.3 Ignition of adjacent materials

Electrical equipment shall not cause ignition of adjacent materials.

3.3.6.14.4 Accidental contact with electrical equipment

Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.

APPENDIX B: GLOSSARY OF TERMS

DEFINITIONS

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or major ground facility. For safety failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.

Credible failure - A condition that has a potential of occurring based on actual failure modes in similar systems.

Critical Hazard - Any condition which may cause a nondisabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system, or involves damage to Orbiter or a ground facility. For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the critical path for station survival or which can be restored through contingency repair.

Design for Minimum Risk - Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance. criteria. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance must be imposed upon external system that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure of the pressure vessel. Examples are mechanisms, structures, glass, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Hazard - The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Hazard Controls - Design or operational features used to reduce the likelihood of occurrence of a hazardous effect. Hazard controls are implemented in the following order of precedence:

a. Elimination of hazard through removal of hazardous sources and operations.

b. Ensure inherent safety through provisions of appropriate design features, materials and parts selection, and safety factors. Design considerations to include damage control, containment, isolation of potential hazards and failure tolerance considerations.

c. Reduce hazard to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

d. Minimize the effects of potential hazards through the use of warning devices, crew operational procedures or protective clothing and/or equipment.

Hazardous command - A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard.

Independent inhibit - Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

Independent Safing Action - A safing action is an action generated by a nonfailed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent both safing actions from transitioning the system to a safe state.

Inhibit - a. Hardware implementation: A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.). b. Software implementation: A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available. Note: Software inhibits are not counted in meeting safety requirements for multiple inhibits.

Interlock - A design feature that ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed.

Local control - A capability to accomplish a function at the direction of the crew within the applicable on-orbit module and also prevent reconfiguration of the function by an external entity during the specified period.

Near Real Time Monitoring - Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). The capability of the hardware and software to provide the updated data for near real-time monitoring data is generally the lowest

available frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Operator error - An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

Rapid Safing - The capability of the Orbiter to accomplish an emergency deorbit or a deobit contingency to the next primary landing site.

Radiation, Ionizing - TBD

Radiation, ionizing - TBD

Real Time Monitoring - Notification of changes in inhibit or safety status to the crew at a rate adequate to allow for appropriate reaction to a change in the status. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user to react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

Safe - A general term denoting an acceptable level of risk, relative freedom from and low probability of: personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

Safety critical - A condition, event, operation, process, function, equipment or system (including software and firmware) with potential for personnel injury or loss, or with potential for loss or damage to vehicles, equipment or facilities, loss or excessive degradation of the function of critical equipment, or which is necessary to control a hazard.

Safety critical software - Software which:

a. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly, could result in control function loss or error which could cause a hazard

b. Monitors the condition or state of hardware components and, if monitoring is not performed or is performed incorrectly, could provide data which results in erroneous operator or companion system decisions which could cause a hazard

c. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly in conjunction with human error or hardware failure, could cause a hazard.

Safing - Event or sequence of events necessary to place systems, subsystems or component parts into predetermined safe conditions.

APPENDIX F - Italian Mini-Pressurized Logistics Segment Specification

3.3.6 Safety.

3.3.6.1 General

3.3.6.1.1 Catastrophic Hazards

The MPLM shall be designed such that no combination of two failures, or two operator errors (See 6.1), or one of each can result in a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or a major ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls (See 6.1) at the Segment/System levels.

3.3.6.1.2 Critical Hazards.

The MPLM shall be designed such that no single failure or single operator error can result in a nondisabling personnel injury, severe occupational illness; loss of a major ISS element on-orbit life sustaining function or emergency system, or involves damage to the Orbiter or a ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.3 Design for minimum risk.

Hazards related to ”Design for Minimum Risk” (See 6.1) areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of ”Design for Minimum Risk” areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards.

3.3.6.1.4.1 Inadvertent operation resulting in critical hazards.

A function whose inadvertent operation could result in a critical hazard (See 6.1) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of function resulting in critical hazards.

Where loss of a function could result in a critical hazard, no single credible failure (See 6.1) shall cause loss of that function. The function shall be monitored such that the necessary safety data that require operator or automated action for safing is acquired prior to the time to critical hazardous effects. Where operator input to control the hazard would be untimely or ineffective, the MPLM shall have the capability to automatically safe the function prior to the time to critical hazardous effect. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels **(TBR)**.

3.3.6.1.5 Control of functions resulting in catastrophic hazards.

3.3.6.1.5.1 Inadvertent operation resulting in catastrophic hazards

Compliance with requirements a, b and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See 6.1), whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in catastrophic hazards

Compliance with requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

b. The function shall be monitored such that necessary safety data that require operator or automated action for safing is acquired prior to the time to catastrophic hazardous effects. Where operator input to control the hazard would be untimely or ineffective, the MPLM shall have the capability to automatically safe the function prior to the time to catastrophic hazardous effect. **(TBR)**.

3.3.6.1.6 Subsequent induced loads

If a component of the MPLM is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the component to eliminate the hazard.
MPLM responsibility would be to define the minimum interface configuration that must be maintained during specific flight phases to avoid hazardous consequences.

3.3.6.1.7 Safety interlocks.

Safety interlocks (See 6.1) shall be provided to prevent unsafe operations when access to MPLM equipment is required for maintenance for ground operation.

3.3.6.1.8 Environmental compatibility.

MPLM functions shall be safe (See 6.1) in the applicable worst case natural and induced environments defined in paragraph 3.2.6 "Environmental Conditions" or as defined in a payload integration plan , mission integration plan and/or interface control document.

3.3.6.2 Hazard Detection and Safing

3.3.6.2.1 Reserved.

3.3.6.2.2 Monitors.

3.3.6.2.2.1 Status information

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention

Monitor devices shall be current limited or otherwise designed such that credible failures (shorts) will not operate the hazardous function.

3.3.6.2.2.3 Loss of input or failure

Loss of input or failure of the monitor shall be identifiable.

3.3.6.2.2.4 Launch site availability

Monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 Flight crew availability

Notification of changes in the status of safety monitoring shall be available to the flight crew in either near-real time or real time monitoring.

3.3.6.2.3 Near-real time monitoring.

Near-real time monitoring (See 6.1) of inhibits shall be required for systems with potential hazardous functions not real-time monitored. Failure reporting will be in accordance with the ISS capability, such that the necessary safety data that require operator or automated action for safing is acquired prior to the time to hazardous effects. The frequency of the monitoring is generally the lowest available with normal telemetry, but will be determined on a case by case basis depending on the time to effect of the hazard **(TBR)**.

3.3.6.2.4 Real Time Monitoring.

3.3.6.2.4.1 Maintain status of hazard controls

The MPLM shall provide real-time monitoring (See 6.1) to catastrophic hazardous functions to maintain status of hazard controls when the crew or the MPLM is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground monitoring

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within time to effect of the hazard upon loss of communications with the ground.

3.3.6.3 Command and computer control of hazardous functions

3.3.6.3.1 Computer control of hazardous functions

The computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038B **(TBR)**.

3.3.6.4 Hazardous Materials

3.3.6.4.1 Hazardous fluid containment failure tolerance.

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate with the hazard level or be contained in an approved pressure vessel as defined in SSP 30558.

3.3.6.4.2 Reserved

3.3.6.5 Pyrotechnics. - Reserved

3.3.6.6 Radiation

3.3.6.6.1 Nonionizing Radiation. - Reserved

3.3.6.6.2 MPLM Transmitters. - Reserved

3.3.6.6.3 Ionizing Radiation Crew Limits

The design of the MPLM shall limit the ionizing radiation dose in habitable volumes to 40 rem (BFO) per year.

3.3.6.7 Optics and Lasers. - Reserved

3.3.6.8 Electrical Safety

3.3.6.8.1 Electrical power circuit overloads.

3.3.6.8.1.1 Circuit overload protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B 3.5.2 (Wire and Cable Derating) are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination

a. MPLM electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

b. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock.

The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3.

3.3.6.8.3 Reapplication of power.

The MPLM shall provide means for Station control of interruption and reapplication of power to each refrigerator/freezer (R/F) interface

3.3.6.8.4 Batteries.

Batteries shall be designed to control application hazards caused by buildup or venting of flammable, corrosive or toxic gasses and reaction products; the expulsion of electrolyte; and by failure modes of over temperature, shorts, reverse current, cell reversal, leakage, cell grounds, and over pressure. Safety guidelines for batteries are contained in NSTS 20793.

3.3.6.9 Cryogenics. - Reserved.

3.3.6.10 Fire protection

3.3.6.10.1 Manual activation. - Reserved.

3.3.6.10.2 Isolation.

The MPLM shall ensure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.

3.3.6.10.3 Suppression.

The MPLM Flight System shall accommodate the application of a fire suppressant at each location containing a potential fire source.

3.3.6.10.4 Suppressant

The release of CO2 suppressant into the Manned MPLM shall not raise the atmosphere CO2 concentration above 34.2 mm-Hg partial pressure.

3.3.6.10.5 Restorable suppression.

Fixed fire suppression, where installed, shall be restorable after discharge.

3.3.6.10.6 Power Removal

Fixed fire suppression, where installed, shall remain functional after the removal of power to a location after detection of a fire event.

3.3.6.10.7 Portable equipment.

3.3.6.10.7.1 Set co-location

One PBA and PFE shall be located in the MPLM Flight System. The PBA and PFE shall be located within three (3) feet of each other. PBA and PFE installation shall be in accordance with SSP 30257:008 and SSP 30262:010 respectively.

3.3.6.10.8 Loss of detection.

The MPLM shall ensure that no single failure causes loss of detection of fire events in locations where a loss of functionality may create a catastrophic hazard.

3.3.6.10.9 Confirmation

The MPLM shall confirm a fire event condition prior to any automated isolation, or suppression. Confirmation consists of at least two validated indications of fire/smoke from a detector.

3.3.6.11 Constraints

3.3.6.11.1 Reserved

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance.

3.3.6.11.2.1 Pressure differential tolerance

MPLM equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard .

3.3.6.11.2.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards.

3.3.6.11.3. Emergency egress.

The MPLM shall provide for safe emergency IVA egress to the remaining contiguous pressurized volumes and have the capability to isolate from other flight pressurized volumes within three minutes, including closing hatches.

3.3.6.11.4. Reserved.

3.3.6.11.5 Reserved.

3.3.6.11.6 Component hazardous energy provision.

Components, which retain hazardous energy potential shall either be designed to prevent a crewmember conducting maintenance from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful.

3.3.6.11.7 Hatch opening.

The MPLM shall support the capability to control pressure differential providing the PEV as part of the Hatch (common to ISS) The MPLM shall provide a sampling interface to allow collection of MPLM atmosphere prior to crew ingress. Visual inspection of the interior of MPLM prior to crew ingress is via the Hatch window.

3.3.6.11.8 Reserved.

3.3.6.11.9 Reserved.

3.3.6.11.10 Reserved.

3.3.6.11.11 Reserved.

3.3.6.11.12 Hazardous Gas Accumulation.

3.3.6.11.12.1 Accumulation prevention

The MPLM shall provide the capability to prevent uncontrolled hazardous accumulations of gases.

3.3.6.11.12.2 Detection, monitoring, and control. - Reserved

3.3.6.11.13 Equipment clearance for entrapment hazard.

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Light Fixture.

Light fixtures assemblies shall incorporate features to contain all glass fragments in the case of lamp breakage.

3.3.6.11.15 Reserved.

3.3.6.12 Human engineering safety

3.3.6.12.1 Internal volume touch temperature.

3.3.6.12.1.1 Continuous contact - high temperature

Surfaces which are subject to continuous contact with crewmember bare skin and whose temperature exceeds 113 degrees Fahrenheit, shall be provided with guards or insulation to prevent crewmember contact.

3.3.6.12.1.2 Incidental or momentary contact - high temperature

For incidental or momentary contact (30 seconds or less), the following apply:

Crewmember warning - Surfaces which are subject to incidental or momentary contact with crewmember bare skin and whose temperatures are between 113 and 122 degrees Fahrenheit shall have warning labels that will alert crewmembers to the temperature levels.

Crewmember protection - Surface temperatures which exceed 122 degrees Fahrenheit shall be provided with guards or insulation that prevent crewmember contact.

3.3.6.12.1.3 Internal volume low touch temperature

When surfaces below 39 degrees Fahrenheit which are subject to continuous or incidental contact, are exposed to crewmember bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site.

3.3.6.12.2 External touch temperature.

The suit shall be protected from high or low touch temperature extremes as follows:

3.3.6.12.2.1 Incidental contact

For incidental contact, temperatures shall be maintained within -180 to +235 degrees F, or limit heat transfer rates as specified in Table 2.

TABLE 2. Heat transfer rates				
Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate(1) (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52(2)
	Incidental (0.5 max)	113	1.444	176.2(3)
Cold Object	Unlimited	40	1.062	-132.7(2)
	Incidental (0.5 max)	40	1.478	-325.2(3)

Notes:
1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

3.3.6.12.2.2 Unlimited contact

For unlimited contact, temperatures shall be maintained within -45 degrees F to +145, or for designated EVA crew interfaces specified in Table 3, limit heat transfer rates as specified in Table 2.

TABLE 3. Designated EVA interfaces
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection.

3.3.6.12.3.1 Sharp edges

MPLM equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall protect the crew from injury due to sharp edges by the use of corner and edge guards or by rounding the corners and edges in accordance with NSTS 07700, Vol. XIV, Appendix 7, Paragraph 2.3, Crew and equipment safety, and Tables II.2-IIa and II.2-IIb.

3.3.6.12.3.2 Thin materials

Materials less than 0.08 inches thick, with exposed edges that are uniformly spaced, not to exceed 0.5 inch gaps, flush at the exposed surface plane and shielded from direct EVA interaction, shall have edge radii greater than 0.003 inches.

3.3.6.12.3.3 Planned maintenance or storage. - Reserved

3.3.6.12.4 Internal corner and edge protection.

3.3.6.12.4.1 Equipment exposed to crew activity

Surfaces of MPLM equipment and ORUs located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraphs 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3, Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 Equipment exposed only during planned maintenance activities. - Reserved

3.3.6.12.5 Reserved

3.3.6.12.6 Latches.

Latches or similar devices shall be designed to prevent entrapment of crewmember appendages.

3.3.6.12.7 Screws and bolts.

Screws or bolts, except internal ORU screws and bolts, in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 in. in length shall have protective features to prevent snagging, to protect against sharp edges, and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 Safety Critical Fasteners

Safety critical fasteners shall be designed to prevent inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls.

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

3.3.6.12.10 Burrs.

Exposed surfaces shall be smooth and free of burrs.

3.3.6.12.11 Holes

3.3.6.12.11.1 Equipment located inside habitable volumes

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside habitable volumes.

3.3.6.12.11.2 Equipment located outside habitable volumes

Holes (round, slotted, polygonal) in EVA translation, when handrails/holds are used, shall be 1.0 inches or greater in diameter.

3.3.6.12.12 Protrusions.

Equipment except for translation aids identified in Table 3 shall not protrude into the 50 inch horizontal by 72 inch vertical envelope of the CETA/MT corridor, or the 43 inch horizontal envelope of the primary and secondary translation path.

3.3.6.12.13 Pinch points.

Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crewmember appendages.

3.3.6.12.14 Emergency Ingress. - Reserved

3.3.6.12.15 Reserved

3.3.6.12.16 Flexhoses.

Flexhoses and lines with delta pressure shall be restrained or otherwise captured to prevent injury to crew and/or damage to adjacent hardware.

3.3.6.12.17 Translation routes and established worksites.

For protection from hazards along translation routes and established worksites the following apply:

3.3.6.12.17.1 Primary translation routes and established worksites

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.

b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.17.2 Secondary translation routes and established worksites

External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded and controlled as specified in Table 4.

TABLE 4. Control for exposed risks to EVA crew

Risk Type	Hazard	Control Method *
Innate Characteristics	Non-Ionizing Radiation (Antennas transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards
	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Connectors	Warning Strips and Placards
	Thermal (>235 degrees F or < -180 degrees F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards

	Narrow Passageways Protrusions	Placards
	Structure Sensitive to EVA Loads	Placards
	Pinch Points	Placards
	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards
CETA Corridor	Structural Impacts - Mobile Transporter - End of Rail	Color-coded Anodized yellow with black cross-hatching
Note: * Control methods shall be designed in accordance with SSP 50006.		

3.3.6.12.17.3 EVA crewmember contact isolation

MPLM hardware which cannot be controlled by design features to comply with ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crewmember contact.

3.3.6.12.18 Moving or rotating equipment.

The EVA crewmember shall be protected from moving or rotating equipment.

3.3.6.13 Launch vehicle interfaces and services.

3.3.6.13.1 Safe Without Space Shuttle Program Services.

3.3.6.13.1.1 Fault tolerance/safety margins

The MPLM shall maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight Space Shuttle Program services.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions

During Orbiter emergency conditions, MPLM shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter Services.

When Orbiter services are to be utilized to control MPLM hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of functions resulting in critical hazards and 3.3.6.1.5, Control of functions resulting in catastrophic hazards.

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions

Inadvertent deployment, separation or jettison of the MPLM or appendages which could result in a collision or inability to sustain subsequent loads shall be one or two failure tolerance consistent with the hazard level. The general inhibit and monitoring requirements of 3.3.6.1.4, 3.3.6.1.5 and 3.3.6.2.2 apply **(TBR)**.

3.3.6.13.4 Planned Deployment/Extension Functions

3.3.6.13.4.1 Violation of Orbiter payload door envelope

If a component of the MPLM or any MPLM orbital support equipment (OSE) violates the payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance

The combination of these primary and backup methods shall be two-fault tolerant. Two methods are considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency Return and Rapid Safing.

The MPLM shall be designed such that it does not preclude the Orbiter from safing the payload bay for door closure and deorbit when emergency conditions develop. For emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes. For a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements apply to MPLM hardware with direct interfaces with the Orbiter:

3.3.6.13.5.1 Emergency deorbit

The MPLM hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-MPLM hardware operations.

3.3.6.13.5.2 Next primary landing site contingency deorbit

The MPLM hardware shall have a single failure tolerant capability to allow the Orbiter to meet next primary landing site contingency deorbit requirements. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-MPLM hardware operations.

3.3.6.13.6 Flammable Atmosphere.

3.3.6.13.6.1 Normal functions

During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) MPLM functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical ignition sources

Electrical ignition sources shall not be exposed.

3.3.6.13.6.3 Surface temperatures

Surface temperatures shall be below 352 degrees F.

3.3.6.13.6.4 Conductive surfaces

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1 **(TBR)**.

3.3.6.13.7 Allowable RF radiation levels. - Reserved

3.3.6.13.8 Lightning protection

MPLM electrical circuits may be subjected to the electromagnetic fields described in NSTS 07700, Volume XIV, Attachment 1 due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard **(TBR)**.

3.3.6.13.9 Orbiter vent/dump provisions

3.3.6.13.9.1 Release or ejection of hazardous material

MPLM hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS.

3.3.6.13.9.2 Fluid system containment

MPLM shall be designed to contain both hazardous and nonhazardous fluids when in the presence of the Orbiter.

3.3.6.13.10 Sealed Compartments.

MPLM components, located in regions of the Orbiter other than the habitable volume, shall be designed to withstand the decompression and repressurization enviroments associated with ascent or descent without resulting in a hazard.

3.3.6.14 Ground interfaces and services - Space Shuttle launch

Hazards shall not be created due to the inaccessibility of flight hardware such as:

3.3.6.14.1 Moving parts

Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.

3.3.6.14.2 Equipment requiring adjustment

Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable.

3.3.6.14.3 Ignition of adjacent materials

Electrical equipment shall not cause ignition of adjacent materials.

3.3.6.14.4 Accidental contact with electrical equipment

Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.

APPENDIX B: GLOSSARY OF TERMS

DEFINITIONS

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or major ground facility. For safety failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.

Credible failure - A condition that has a potential of occurring based on actual failure modes in similar systems.

Critical Hazard - Any condition which may cause a nondisabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system, or involves damage to Orbiter or a ground facility. For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the critical path for station survival or which can be restored through contingency repair.

Design for Minimum Risk - Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance. criteria. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance must be imposed upon external system that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure of the pressure vessel. Examples are mechanisms, structures, glass, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Hazard - The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Hazard Controls - Design or operational features used to reduce the likelihood of occurrence of a hazardous effect. Hazard controls are implemented in the following order of precedence:

a. Elimination of hazard through removal of hazardous sources and operations.

b. Ensure inherent safety through provisions of appropriate design features, materials and parts selection, and safety factors. Design considerations to include damage control, containment, isolation of potential hazards and failure tolerance considerations.

c. Reduce hazard to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

d. Minimize the effects of potential hazards through the use of warning devices, crew operational procedures or protective clothing and/or equipment.

Hazardous command - A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard.

Independent inhibit - Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

Independent Safing Action - A safing action is an action generated by a nonfailed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent both safing actions from transitioning the system to a safe state.

Inhibit - a. Hardware implementation: A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.). b. Software implementation: A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available. Note: Software inhibits are not counted in meeting safety requirements for multiple inhibits.

Interlock - A design feature that ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed.

Local control - A capability to accomplish a function at the direction of the crew within the applicable on-orbit module and also prevent reconfiguration of the function by an external entity during the specified period.

Near Real Time Monitoring - Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). The capability of the hardware and software to provide the updated data for near real-time monitoring data is generally the lowest available frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Operator error - An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

Rapid Safing - The capability of the Orbiter to accomplish an emergency deorbit or a deobit contingency to the next primary landing site.

Real Time Monitoring - Notification of changes in inhibit or safety status to the crew at a rate adequate to allow for appropriate reaction to a change in the status. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user to react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

Safe - A general term denoting an acceptable level of risk, relative freedom from and low probability of: personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

Safety critical - A condition, event, operation, process, function, equipment or system (including software and firmware) with potential for personnel injury or loss, or with potential for loss or damage to vehicles, equipment or facilities, loss or excessive degradation of the function of critical equipment, or which is necessary to control a hazard.

Safety critical software - Software which:

a. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly, could result in control function loss or error which could cause a hazard

b. Monitors the condition or state of hardware components and, if monitoring is not performed or is performed incorrectly, could provide data which results in erroneous operator or companion system decisions which could cause a hazard

c. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or if performed out of sequence or incorrectly in conjunction with human error or hardware failure, could cause a hazard.

Safing - Event or sequence of events necessary to place systems, subsystems or component parts into predetermined safe conditions.

APPENDIX G - MOBILE SERVICING SYSTEM SEGMENT SPECIFICATION

3.3.6.1 General

3.3.6.1.1 Catastrophic Hazards (See 6.1)

The MSS shall be designed such that no combination of two failures, two operator errors (See 6.1), or one of each can result in a disabling or fatal personnel injury, or loss of one of the following: Orbiter, ISS, or a major ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls (See 6.1) at the Segment/System levels.

3.3.6.1.2 Critical Hazards (See 6.1)

The MSS shall be designed such that no single failure or single operator error can result in a non disabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system; or involves damage to a launch or servicing vehicle, the Orbiter or a ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of controls at the Segment/System levels.

3.3.6.1.3 Design for minimum risk

Hazards related to ”Design for Minimum Risk” (See 6.1) areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety, that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of ”Design for Minimum Risk” areas of design are components or elements of mechanisms in critical applications, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards (See 6.1)

3.3.6.1.4.1 Inadvertent operation resulting in a critical hazard.

A function whose inadvertent operation could result in a critical hazard (See 6.1) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance

with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of a function resulting in a critical hazard.

Where loss of a function could result in a critical hazard, no single credible failure (See 6.1) shall cause loss of that function. The function shall be monitored such that necessary safety data that require operator or automated action for safing is acquired prior to the time to critical hazardous effects. Where operator input to control the hazard would be untimely or ineffective, the MSS shall have the capability to automatically safe the function prior to the time to critical hazardous effect. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards

3.3.6.1.5.1 Inadvertent operation resulting in a catastrophic hazard.

Compliance with requirements a, b, and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See 6.1) , whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function, (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in a catastrophic hazard

Compliance with the requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of a function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

b. The function shall be monitored such that necessary safety data that require operator or automated action for safing is acquired prior to the time to catastrophic hazardous

effects. Where operator input to control the hazard would be untimely or ineffective, the MSS shall have the capability to automatically safe the function prior to the time to catastrophic hazardous effect.

3.3.6.1.6 Subsequent induced loads

If a component of the MSS is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the MSS component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the MSS component to eliminate the hazard.

3.3.6.1.7 Safety interlocks

Safety interlocks (see 6.1) shall be provided to prevent unsafe operations when access to MSS equipment is required for maintenance.

3.3.6.1.8 Environmental compatibility

MSS functions shall be certified safe (6.1) in the applicable worst case natural and induced environments defined in paragraph 3.2.6, Environmental conditions.

3.3.6.2 Hazard Detection and Safing

3.3.6.2.1 Reserved .

3.3.6.2.2 Safety Monitors

3.3.6.2.2.1 Status information

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention

Monitor circuits shall be current limited or otherwise designed such that credible failures, such as a short circuit, will not operate the hazardous function**.**

3.3.6.2.2.3 Loss of input or failure

Loss of input or failure of the monitor shall cause a change in the state of the indicator.

3.3.6.2.2.4 Launch site availability

Monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 Flight crew availability

Notification of changes in the status of safety monitors shall be available to the flight crew in either near-real time or real time.

3.3.6.2.3 Near-real time monitoring

Inhibits to hazardous functions that require monitoring shall be monitored in near-real time unless there is a specific requirement for the inhibits to be monitored in real time. Failure reporting will be in accordance with the ISS capability, such that necessary safety data that require operator or automated action for safing is acquired prior to the time to hazardous effects.. The frequency of monitoring is generally the lowest available with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

3.3.6.2.4 Real Time Monitoring

3.3.6.2.4.1 Maintain status of hazard controls

The MSS shall provide real-time monitoring (6.1) to catastrophic hazardous functions to maintain status of hazard controls when the crew or MSS is performing a task required for a hazard control. When RTM is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures

If the crew is used is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground Monitoring -Reserved

3.3.6.3 Command and Computer control of hazardous functions

3.3.6.3.1 Computer control of Hazardous Functions

Computer control of hazardous functions shall comply with the safety implementation requirements as specified in SSP 50038A. **(TBD applicability matrix) (SSP 50038B - TBR)**

3.3.6.3.1.1 Detection and Recovery

A computer-based control system shall be designed such that a failure or operator error shall be detected, contained and recovered from such that catastrophic and critical hazardous events are prevented from occurring.

TABLE 3.3.6.3 SEGMENT REQUIREMENTS APPLICABILITY MATRIX (Sheet 1 of 3)

REQUIREMENT	CSA MSS
3.1.1 A computer-based control system shall be designed such that failures or operator errors shall be detected, contained and recovered from to the extent that no combination of two failures, or two operator errors, no one of each will cause a catastrophic hazardous event, or no single failure or operator error will cause a critical hazardous event.	x
3.1.2 A computer-based control system shall be designed such that the detection of a failure that could cause a hazard shall result in a safing action independent from the failure.	x
3.1.3.1 A computer-based control system shall utilize Fault Containment Regions (FCRs) to ensure that a fault does not remove more than one method of hazard control for a hazardous function.	x
3.1.3.2 Computer-based control systems that must be re-configured to provide capability for continued safety critical operations after a fault is detected and contained shall provide the capability to re-configure in a time frame adequate for hazard control..	x
3.1.3.3 A computer-based control system controlling hazardous functions shall have a minimum of two FCRs for critical hazards and three for catastrophic hazards	x
3.1.3.4 A single FCR shall not independently control more than one of the system hazard controls.	x
3.1.3.5 For the control of hazardous functions, a computer-based control system shall use multiple FCRs with uniqueness in functionality and implementation for hazard control.	x
3.2.1.1 Prerequisite conditions for the safe execution of an identified hazardous command shall be met before execution.	x
3.2.1.2 In the event that prerequisite condition have not been met, the software shall reject the command.	x
3.2.1.3 Hazardous commands shall be issued only by a single controlling software function the crew or the ground.	x
3.2.1.4 The initiating crew or ground operator shall be notified upon execution of a hazardous command or provided notification of failure to execute a hazardous command.	x
3.2.1.5 If loss of capability could cause a critical hazard, at least two independent command messages shall be required to cause loss or inadvertent activation of that	x

capability.	
3.2.1.5.1 If loss of a capability could cause a catastrophic hazard, at least two independent command messages shall be required to cause loss of any redundant function within that capability, and at lease three command messages shall be required to cause total loss of that capability.	
3.2.1.5.2 If loss of capability could cause a catastrophic hazard, at least three independent command messages shall be required to cause loss of that capability when a redundant function is not available.	
3.2.1.6 Override commands shall require at least two independent actions by the operator.	x
3.2.1.7 Software shall require two independent actions by the operator to initiate a system function that could result in a catastrophic hazard.	x
3.2.1.8 Software shall require three independent actions by the operator to initiate or terminate a system function that could result in a catastrophic hazard.	x

TABLE 3.3.6.3 SEGMENT REQUIREMENTS APPLICABILITY MATRIX (SHEET 2 OF 3)

REQUIREMENT	**CSA MSS**
3.2.2.1 Software shall make available to the crew and ground operators the status of software inhibits associated with hazardous commands.	x
3.2.2.2 Software inhibits that are bypassed or changed by an override shall be restored to the original state.	
3.2.3.1 Software shall make available to the crew and ground operators the status of software controllable inhibits.	x
3.2.3.2 Software shall provide independent and unique commands to control each software controllable inhibit.	x
3.2.4.1 The Station software shall allow only authorized access.	x
3.2.4.2 Software shall provide proper sequencing of safety critical commands.	x
3.2.4.3 Software shall provide for crew and ground termination or disabling of automatic safing functions.	
3.2.5.1 Hazardous processes and safing processes with a time to criticality, such that timely human intervention may not be available, shall be automated.	x
3.2.5.2 Software shall provide error handling to support safety critical functions.	x
3.2.5.3 Software shall initialize, start and restart components to a known safe state.	x
3.2.5.4 Software termination shall result in a known safe state.	x
3.2.5.5 Software Power On Self Test (POST) shall be confined to that single system process controlled by the component undergoing POST.	x
3.2.5.6 Software Power On Self Test (POST) utilized within any component shall terminate in a known safe state.	x
3.2.5.7 Station core software shall process the received hazardous payloads status and data to provide status monitoring for downlink and failure annunciation to the crew. (Hazardous payloads will automatically provide failure status and data to Station core software systems).	
3.2.5.8 Unused or undocumented code shall be incapable of producing a critical or catastrophic hazard.	x
3.3 Computer-based control system hardware shall continue to operate nominally during off-nominal power conditions, or contain design features which safe the computer-based control system and the end functions during off-nominal power conditions.	x
3.4 For software which will interface directly with flight software or directly with test	

and verification software, errors in flight software shall be detected and recovered from such that catastrophic and critical hazardous events are prevented from occurring during execution of the flight software. This applies to the Mission Build Facility.

TABLE 3.3.6.3 SEGMENT REQUIREMENTS APPLICABILITY MATRIX (SHEET 3 OF 3)

REQUIREMENT	CSA/MSS
APPENDIX C-1 COMPUTER-BASED CONTROL SYSTEM REQUIREMENTS	
3.2.4.3.4 The ISS shall provide automatic failure isolation to the level needed for functional recovery of equipment(hardware and software) that supports functions required for 24 hour autonomous operations(listed in Table 3-IV of SSP 41000D). 3.2..4.3.6 The ISS shall automatically confirm restoration of functional performance after automatic functional recovery action. 3.2.1.1.1.7 The Space Station shall classify these abnormal events as Class 1, 2 or 3 alarms for annunciation to the Space Station operators. The on-orbit Space Station shall make the status assessment and alarm event data available to external systems and other capabilities within the Space Station system.	
The on-orbit Space Station shall make the status assessment and alarm event data available to external systems and other capabilities within the Space Station system. 3.2.4.3.8 The ISS shall detect and isolate out-of-tolerance conditions, functional anomalies, and functional operations that may manifest a catastrophic or critical hazard within 24 hours without removal of equipment from its operating location or use of ancillary test equipment.	x
3.2.4.3.9 The ISS shall resolve failure isolation ambiguities functions listed in Table III to the following: A. 90% of identified failure ,modes to one on-orbit maintainable unit. B. 95% of identified failure ,modes to two on-orbit maintainable unit. C. 98% of identified failure ,modes to three on-orbit maintainable unit.	
APPENDIX C-2 OTHER COMPUTER-BASED CONTROL SYSTEM REQUIREMENTS	
(1) Failure, Detection, Isolation, and Recovery (FDIR) switchover software shall be resident on an available, non-failed control platform Orbital Replacement Unit (ORU), which is different from the one with the function being monitored.	x
(2) Software shall accept and process crew, ground operators or executive software commands to activate/deactivate software controllable inhibits.	x
(3) All software inhibits associated with a hazardous command shall have a unique identifier. (This requirement was covered in the Naming Implementors Agreement).	
(4) Each software inhibit command associated with a hazardous command shall be consistently identified using rules and legal values as specified in the Naming Implementors Agreement. (5) If an automated sequence is already running when a software inhibit associated with a hazardous command is activated, the sequence shall complete before the	

software is executed.

NOTE: X -- DESIGNATES ACCEPTANCES/AGREEMENT TO REQUIREMENT

3.3.6.3.1.2 Independent Safing Action

A computer-based control system shall be designed such that the detection of a failure that could cause a hazard shall result in an independent safing action **(6.1)** .

3.3.6.4 Hazardous materials

3.3.6.4.1 Hazardous fluid containment failure tolerance -Reserved

3.3.6.4.2 Storage of Hazardous Chemicals - Reserved

3.3.6.5 Pyrotechnics - Reserved

3.3.6.6 Radiation

3.3.6.6.1 Non ionizing Radiation

a. The MSS shall limit the levels of non ionizing radiation of the MSS in accordance with SSP 50005, paragraphs 5.7.3.2 and 5.7.3.2.1 to provide personnel protection.

3.3.6.7 Optics and Lasers. - Reserved

3.3.6.8 Electrical Safety

3.3.6.8.1 Electrical power circuit overloads

3.3.6.8.1.1 Circuit overload protection

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing

Circuit protective devices shall be sized such that steady state currents in excess of the values allowed by SSP 30312, Appendix B, Section B3.5.2 (Wire and Cable Derating) are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination

a. MSS electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function.

b. Conductive contamination shall not cause shorts between conductors within a connector that cause the removal of more than one inhibit to a hazardous function.

3.3.6.8.2 Crew protection for electrical shock

The crew shall be protected from electrical hazards in accordance with SSP 50005, Section 6.4.3.

3.3.6.8.3 Reapplication of power - Reserved

3.3.6.8.4 Batteries - Reserved

3.3.6.9 Propulsion - Reserved

3.3.6.10 Fire Protection - Reserved

3.3.6.11 Constraints

3.3.6.11.1 Reserved

3.3.6.11.2 Pressurized volume depressurization and repressurization tolerance

3.3.6.11.2.1 Pressure differential tolerance

MSS equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard

3.3.6.11.2.2 Operation during pressure changes - Reserved

3.3.6.11.3 Emergency Egress - Reserved

3.3.6.11.4 Reserved

3.3.6.11.5 Reserved

3.3.6.11.6 Component hazardous energy provision.

Components, which retain hazardous energy potential, shall be designed to prevent a crew member, conducting maintenance, from releasing the stored energy potential or be designed with provisions to allow safing of the potential energy including provisions to confirm that the safing was successful.

3.3.6.11.7 Hatch Opening - Reserved

3.3.6.11.8 Reserved

3.3.6.11.9 Reserved

3.3.6.11.10 Reserved

3.3.6.11.11 Reserved

3.3.6.11.12 Hazardous Gas Accumulation - Reserved

3.3.6.11.13 Equipment clearance for entrapment hazard

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.14 Light Fixture

Light fixtures shall incorporate features to contain glass fragments 500 microns or larger in size in the case of lamp breakage.

3.3.6.12 Human Engineering Safety

3.3.6.12.1 Internal volume touch temperature

The crew shall be protected from high and low touch temperature extremes as follows:

3.3.6.12.1.1 Continuous contact - high temperature

Surfaces which are subject to continuous contact with crew member bare skin and whose temperature exceeds 113 degrees Fahrenheit, shall be provided with guards or insulation to prevent crew member contact.

3.3.6.12.1.2 Incidental or momentary contact - high temperature

For incidental or momentary contact (30 seconds or less), the following apply:

Crew member warning - surfaces which are subject to incidental or momentary contact with crew member bare skin and whose temperatures are between 113 and 122 degrees Fahrenheit shall have warning labels that will alert crew members to the temperature levels.

Crew member protection - surface temperatures which exceed 122 degrees Fahrenheit shall be provided with guards or insulation that prevent crew member contact.

3.3.6.12.1.3 Internal volume low touch temperature

When surfaces below 39 degrees Fahrenheit which are subject to continuous or incidental contact, are exposed to crew member bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site.

3.3.6.12.2 External touch temperature

The crew shall be protected from high or low touch temperature extremes as follows:

a. For incidental contact, maintain temperatures within minus 180 to +235 degrees Fahrenheit or limit heat transfer rates as specified in table **TBD-1**.

b. For unlimited contact ~~within designated~~ maintain temperatures within -45 to +145 degrees Fahrenheit; or for designated EVA crew interfaces areas specified in Table **TBD-2,** limit heat transfer rates as specified in table **TBD-1**

TBD-1. Heat transfer rates

Object Temperature	Contact Duration (minutes)	Boundary Node Temperature (5F)	Linear Conductor (BTU/hr 5F)	Maximum Average Heat Rate(1) (Btu/hr)
Hot Object	Unlimited	113	1.149	42.52(2)
	Incidental (0.5 max)	113	1.444	176.2(3)
Cold Object	Unlimited	40	1.062	-132.7(2)
	Incidental (0.5 max)	40	1.478	-325.2(3)

Notes:

1. Positive denotes heat out of the object, negative denotes heat into the object.
2. Averaged over 30 minutes of simulated contact (excursions up to 1.5 times this rate for
3. Averaged over 2 minutes of simulated contact (excursions up to 2.5 times this rate for

TBD-2. Designated EVA interfaces
EVA Tools and Support Equipment
EVA Translation Aids (e.g., CETA Cart, handrails, handholds, etc.)
EVA Restraints (foot restraints, tethers, tether points, etc.)
All EVA translation paths (handrails or structure identified for use as a translation path)
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA worksite accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and Transfer Equipment

3.3.6.12.3 External corner and edge protection

3.3.6.12.3.1. Sharp Edges

MSS equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall provide rounded corners and edges or edge guards in accordance with NSTS 07700 Volume XIV Appendix 7 paragraph 2.3, Crew and Equipment Safety and table II.2a and II.2b

3.3.6.12.3.2 Thin Materials Reserved

3.3.6.12.3.3 Planned Maintenance or Storage

External MSS equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4

3.3.6.12.4 Internal corner and edge protection

3.3.6.12.4.1 Equipment Exposed to Crew Activity

Surfaces of MSS equipment and ORU'S located in pressurized volumes and exposed to crew activity shall protect the crew from injury due to sharp edges and corners within the habitable volume in accordance with SSP 50005, Paragraph 6.3.3.1, Corner and edge requirements for facilities and mounted equipment, 6.3.3.2, Exposed corner requirements from facilities and mounted hardware, 6.3.3.3., Protective covers, and 6.3.3.11, Loose equipment.

3.3.6.12.4.2 Equipment Exposed Only During Planned Crew Maintenance Activities.

Corners and edges of material, equipment or ORUs which are exposed only during planned maintenance activities shall be rounded to a minimum radius or chamfer of 0.03 inches.

3.3.6.12.5 Contingency Repressurization Reserved

3.3.6.12.6 Latches

Latches or similar devices shall be designed to prevent entrapment of crew member appendages.

3.3.6.12.7 Screws and bolts

Screws or bolts except internal ORU screws and bolts in established worksites (planned and contingency) and translation routes (primary and secondary) with exposed threads protruding greater than 0.12 inches in length shall have protective features to prevent snagging, to protect against sharp edges and impact, that do not prevent installation or removal of the fastener.

3.3.6.12.8 Safety Critical Fasteners

Safety Critical Fasteners shall be designed to prevent their inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crew members or their clothing.

3.3.6.12.10 Burrs.

Exposed surfaces shall be smooth and free of burrs.

3.3.6.12.11 Holes

3.3.6.12.11.1 Equipment located inside habitable volumes

Round or slotted holes that are uncovered shall be less than 0.4 inches or greater than 1.0 inches in diameter for equipment located inside the habitable volumes.

3.3.6.12.11.2 Equipment located outside habitable volumes

Holes (rounded, slotted, polygonal) in EVA translation handrails/ hand holes shall be 1.0 inches or greater in diameter.

3.3.6.12.12 Protrusions

Equipment except for translation aids identified in Table XX shall not protrude into the 43 inch cylindrical envelope of the primary and secondary translation path.

3.3.6.12.13 Pinch points

Equipment requiring EVA handling in its final deployment configuration, located outside the habitable volume in translation routes (primary and secondary) and established worksites (planned and contingency), which pivot, retract, or flex such that a gap of greater than 0.5 inches, but less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crew member appendages.

3.3.6.12.14 Emergency Ingress. Reserved

3.3.6.12.15 Reserved

3.3.6.12.16 Flex hoses -

3.3.6.12.17 Translation routes and established worksites

For protection from hazards along translation routes and established worksites the following apply:

3.3.6.12.17.1 Primary translation routes and established worksites

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.
b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.17.2 Secondary translation routes and established worksites

External hardware along secondary translation routes and established worksites posing a risk to EVA crew shall be placarded (See 6.1) and controlled as specified in Table **TBD-3.**

TBD-3. Control for exposed risks to EVA crew/Placards		
Risk Type	Hazard	Control Method *
Innate Characteristics	Non-Ionizing Radiation (Antennas transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards
	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Connectors	Warning Strips and Placards
	Thermal (>235 degrees F or < -180 degrees F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards
	Narrow Passageways Protrusions	Placards
	Structure Sensitive to EVA Loads	Placards
	Pinch Points	Placards
	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards
CETA Corridor	Structural Impacts - Mobile Transporter - End of Rail	Color-coded Anodized yellow with black cross-hatching
Note: * Control methods shall be designed in accordance with SSP 50006.		

3.3.6.12.17.3 EVA crew member contact isolation

MSS hardware which cannot be controlled by design features to comply the ”Primary translation routes and established worksites” or ”Secondary translation routes and established worksites” shall be isolated to preclude EVA crew member contact.

3.3.6.12.18 Moving or rotating equipment

The EVA crew member shall be protected from moving or rotating equipment.

3.3.6.13 Launch vehicle transport - Space Shuttle launch

3.3.6.13.1 Safe Without Space Shuttle Program Services Reserved

3.3.6.13.2 Critical Orbiter Services Reserved

3.3.6.13.3 Inadvertent Deployment, Separation, and Jettison Functions. Reserved

3.3.6.13.4 Planned Deployment / Extension Functions

3.3.6.13.4.1 Violation of Orbiter payload door envelope

If a component of the MSS or any MSS orbital support equipment (OSE) violates the Orbiter payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance

The combination of the primary and backup methods to clear the Orbiter payload door envelope shall be two-fault tolerant. Two methods shall be considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency Return and Rapid Safing

The MSS shall be designed such that it does not preclude the Orbiter from safing the Orbiter payload bay for door closure and deorbit, when emergency conditions develop. These requirements are that: (1) for emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes; and (2) for a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minutes later. The following requirements shall apply to MSS hardware with direct interfaces with the Orbiter:

3.3.6.13.5.1 Emergency deorbit

The MSS hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-MSS hardware operations.

3.3.6.13.5.2 Next primary landing site contingency deorbit

The MSS hardware shall have a single failure tolerant capability to allow the Orbiter to meet the next primary landing site contingency deorbit requirement. When RMS is utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-RS hardware operations.

3.3.6.13.6 Flammable Atmosphere

3.3.6.13.6.1 Normal functions

During Orbiter entry, landing, and post landing operations (whether planned or contingency), the normal (no failures) MSS functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical Interfaces Reserved

3.3.6.13.6.3 Surface temperatures Reserved

3.3.6.13.6.4 Conductive surfaces

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in NSTS 07700, Volume XIV, Attachment 1.

3.3.6.13.7 Allowable RF Radiation Levels Reserved

3.3.6.13.8 Lightning Protection Reserved

3.3.6.13.9 Orbiter / Vent Dump Provisions

3.3.6.13.9.1 Release or ejection of hazardous materials Reserved

3.3.6.13.9.2 Fluid system containment Reserved

3.3.6.13.10 Sealed Containers

MSS components , located in regions of the Orbiter other than the habitable volume, shall be designed to withstand the decompression and recompression environments associated with ascent and descent without resulting in a hazard.

3.3.6.14 Ground interfaces and services - Space Shuttle launch

Hazards shall not be created due to the inaccessibility of flight hardware such as the following:

3.3.6.14.1 Moving parts Reserved

3.3.6.14.2 Equipment requiring adjustment

Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable.

3.3.6.14.3 Ignition of adjacent materials

Electrical equipment shall not cause ignition of adjacent materials.

3.3.6.14.4 Accidental contact with electrical equipment

Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.

3.3.6.15 Ground support equipment safety requirements for Space shuttle launch of MSS hardware.

The MSS ground support equipment designated to be processed at the Space Shuttle launch site shall be in accordance with SSP 50004.

DEFINITIONS

Catastrophic Hazard - Any condition which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the Orbiter, ISS, or major ground facility. For safety failure tolerance considerations, loss of the ISS is be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.

Credible failure - A condition that has a potential of occurring based on actual failure modes in similar systems.

Critical Hazard - Any condition which may cause a nondisabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system; or involves damage to the Orbiter or a ground facility. For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the critical path for station survival or which can be restored through contingency repair.

Design for Minimum Risk - Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance criteria. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance criteria must be imposed upon external systems that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure of the pressure vessel. Examples are structures, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

Hazard - The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

Hazard Controls - Design or operational features used to reduce the likelihood of occurrence of a hazardous effect. Hazard controls are implemented in the following order of precedence:

a. Elimination of the hazard through removal of hazardous sources and operations;

b. Ensure inherent safety through provisions of appropriate design features, materials and parts selection, and safety factors. Design considerations to include damage control, containment, isolation of potential hazards, and failure tolerance considerations.

c. Reduce hazard to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

d. Minimize the effects of potential hazards through the use of warning devices, crew operational procedures or protective clothing and / or equipment.

Hazardous command - A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard such as the removal of a required safety inhibit to a hazardous function..

Impeded -(past tense of impede) - to obstruct or delay the progress of

Independent inhibit - Two or more inhibits are independent if no single credible failure, event or environment can eliminate more than one inhibit.

Independent Safing Action - An independent safing action is an action generated by a non failed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent both safing actions from transitioning the system to a safe state.

Inhibit - A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.).

Interlock - A design feature that ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed.

Local control - A capability to accomplish a function at the direction of the crew within the applicable on-orbit module and also prevent reconfiguration of the function by an external entity during the specified period.

Near Real Time Monitoring - Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). The capability of the hardware and software to provide the updated data for near real-time monitoring data is generally the lowest

available frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

Operator error - An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

Placarded - (past tense of placard) - to post placards on or in. A placard is a printed or written announcement for display in a public place.

Real Time Monitoring - Notification of changes in inhibit or safety status to the crew within a time frame at or near the time the change in status occurred. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user to react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard .

Rapid Safing - The capability of the Orbiter to accomplish an emergency deorbit or a deorbit contingency to the next primary landing site.

Risk - Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

Safe - A general term denoting an acceptable level of risk, relative freedom from and low probability of: personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

Safety critical - A characteristic of a condition, event, operation, process, function, equipment or system (including software and firmware) with potential for personnel injury or loss, or with potential for loss or damage to vehicles, equipment or facilities, loss or excessive degradation of the function of critical equipment, or which is necessary to control a hazard.

Safety Critical software - Software which:
a. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or performed out of sequence or incorrectly, could result in control function loss or error which could cause a hazard.

b. Monitors the condition or state of hardware components and if monitoring is not performed or is performed incorrectly could provide data which results in erroneous operator or companion system decisions which could cause a hazard.
c. Exercises direct command and control over the condition or state of hardware components or software functions and, if not performed or performed out of sequence or incorrectly in conjunction with human error or hardware failure, could cause a hazard.

Safing - An action or sequence of actions necessary to place systems, subsystems or component parts into predetermined safe conditions.

APPENDIX H -Russian Segment Specification

Section 3.3.6

3.3.6 Safety.

3.3.6.1 General.

3.3.6.1.1 Catastrophic Hazards.

The RS shall be designed such that no combination of two failures, two operator errors, or one of each can result in a disabling or fatal flight crew injury, or loss of one of the following: Orbiter, ISS, or a major ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls (See 6.2) at the Segment/System levels.

3.3.6.1.2 Critical Hazards

The RS shall be designed such that no single failure or single operator error can result in a non-disabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system; or involves damage to the Orbiter or a ground facility. Compliance with this requirement may be accomplished at the End Item level or through a combination of controls at the Segment/System levels.

3.3.6.1.3 Design for minimum risk.

Hazards related to ”Design for minimum risk” (See 6.2) areas of design shall be controlled by the safety related properties and characteristics of the design, such as margin or factors of safety,that have been baselined by ISS program requirements. The failure tolerance criteria of paragraphs 3.3.6.1.1 and 3.3.6.1.2 are only to be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. Examples of ”Design to minimum risk” areas of design are mechanisms, structures, glass, pressure vessels, pressurized line and fittings, pyrotechnic devices, material compatibility, material flammability, etc.

3.3.6.1.4 Control of functions resulting in critical hazards.

3.3.6.1.4.1 Inadvertent operation resulting in a critical hazard.

A function whose inadvertent operation could result in a critical hazard (See 6.2) shall be controlled by two independent inhibits, whenever the hazard potential exists. Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.4.2 Loss of a function resulting in a critical hazard.

Where loss of a function could result in a critical hazard, no single credible failure (see 6.2) shall cause loss of that function and the function shall be monitored and controlled in accordance with

ISS capabilities ”Monitor System Status” (paragraph 3.2.1.1.1.7) and ”Respond to Loss of Function” (paragraph 3.2.1.1.1.4). Compliance with this requirement may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

3.3.6.1.5 Control of functions resulting in catastrophic hazards.

3.3.6.1.5.1 Inadvertent operation resulting in a catastrophic hazard.

Compliance with requirements a, b, and c may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. A function whose inadvertent operation could result in a catastrophic hazard shall be controlled by a minimum of three independent inhibits (See 6.2), whenever the hazard potential exists.

b. The return path for the function circuit shall be interrupted by one of the required inhibits if the design of the function circuit without the return path inhibit in place is such that a single credible failure between the last power side inhibit and the function (e.g., a single short to power) can result in inadvertent operation of the catastrophic hazardous function.

c. At least two of the three required inhibits shall be monitored.

3.3.6.1.5.2 Loss of function resulting in a catastrophic hazard.

Compliance with the requirements a and b may be accomplished at the End Item level or through a combination of hazard controls at the Segment/System levels.

a. If loss of the function could cause a catastrophic hazard, no two credible failures shall cause loss of that function.

b. The function shall be monitored and controlled in accordance with ”Monitor system status’ (paragraph 3.2.1.1.1.7) and ”Respond to loss of function” (paragraph 3.2.1.1.1.4).

3.3.6.1.6 Subsequent induced loads.

If a component of the RS is deployed, extended, or otherwise unstowed to a condition where it cannot withstand subsequent induced loads, there shall be one or two-failure tolerant design provisions to safe the RS component appropriate to the hazard level. Safing may include deployment, jettison, or provisions to change the configuration of the RS component to eliminate the hazard.

3.3.6.1.7 Safety interlocks.

Equipment access doors or covers shall incorporate interlocks (See 6.2) to remove all potentials in excess of 200 volts when open.

3.3.6.1.8 Environmental compatibility.

RS functions shall be certified see (6.2) in the worst case natural and induced environments.

3.3.6.1.9 Redundant functions.

Redundant functions that are required to prevent a hazardous event shall be separated to eliminate single failure points from affecting more than one redundant function.

3.3.6.2 Hazard detection and safing.

3.3.6.2.1 Safing prior to return/resupply/refurbishment.

The RS shall incorporate the capability to return systems which are hazardous to a safe condition and to confirm safing prior to being returned, resupplied, or refurbished.

3.3.6.2.2 Monitors.

3.3.6.2.2.1 Status information.

Monitoring circuits shall be designed such that the information is related to the status of the monitored device without compromising or reducing the safety of that monitored device.

3.3.6.2.2.2 Hazardous function operation prevention.

Monitor circuits shall be current limited or otherwise designed such that credible failures, such as a short circuit, will not operate the hazardous function.

3.3.6.2.2.3 Loss of input or failure.

Loss of input or failure of the monitor shall cause a change in the state of the indicator.

3.3.6.2.2.4 Launch site availability.

For RS elements transported by the Orbiter, monitoring shall be available to the launch site when necessary to assure safe ground operations.

3.3.6.2.2.5 Flight crew availability.

Notifications of changes in the status of safety monitoring shall be available to the flight crew in either near real-time or real-time monitoring.

3.3.6.2.3 Near real-time monitoring.

Near real-time monitoring (See 6.2) of inhibits shall be required for systems with potential hazardous functions that are not real-time monitored. Failure reporting will be in accordance with the ISS capability, ”Respond to Loss of Function” (paragraph 3.2.1.1.1.4). The frequency of monitoring is generally the lowest available with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

3.3.6.2.4 Real-time monitoring.

3.3.6.2.4.1 Maintain status of hazard controls.

The RS shall provide real-time monitoring (See 6.2) to catastrophic hazardous functions to maintain status of hazard controls when the crew or RS is performing a task required for a

hazard control. When real-time monitoring is required only for crew involved operations, local visual indicators (including switch talkbacks) are acceptable monitors.

3.3.6.2.4.2 Crew response time and safing procedures.

If the crew is used to provide an operational control to a hazard, adequate crew response time to avoid hazard occurrence and acceptable safing procedures shall be required.

3.3.6.2.4.3 Ground monitoring.

If only ground monitoring is used to meet real-time monitoring, the design shall provide for safing within time to effect of the hazard upon loss of communications with the ground.

3.3.6.3 Command and computer control of hazardous functions.

3.3.6.3.1 Computer control of hazardous functions.

Computer control of hazardous functions with specific hardware and software safety implementation requirements shall be in accordance with the requirements of SSP 50094 **(Paragraph TBD), (SSP 50038B - TBR).**

3.3.6.3.1.1 Detection and recovery.

A computer-based control system shall be designed such that a failure or operator error shall be detected, isolated and recovered from such that catastrophic and critical hazardous events are prevented from occurring.

3.3.6.3.1.2 Independent safing action.

A computer-based control system shall be designed such that the detection of a failure that could cause a hazard shall result in an independent safing action (See 6.2).

3.3.6.4 Hazardous materials.

3.3.6.4.1 Hazardous fluid containment failure tolerance.

Toxic or hazardous chemicals/materials shall have failure tolerant containment appropriate to the hazard level or be contained in an approved pressure vessel as specified in SSP 50094, section 7.0.

3.3.6.4.2 Reserved.

3.3.6.5 Pyrotechnics for RS applications.

The pyrotechnic functions used in applications on RS where failure to fire, inadvertent firing or malfunction during firing may cause hazardous consequences shall be designed in accordance with SSP 50094.

3.3.6.6 Radiation.

3.3.6.6.1 Ionizing radiation.

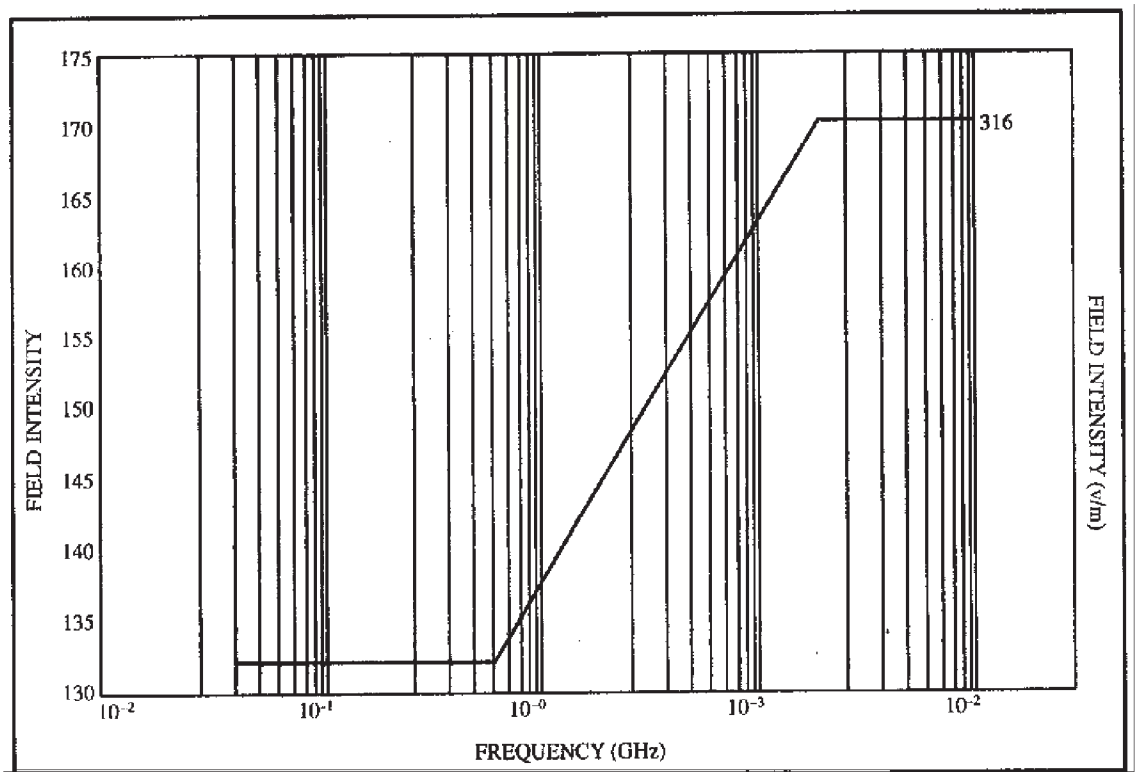
RS components containing or using radioactive materials or that generate ionizing radiation shall be in accordance with SSP 50094.

3.3.6.6.2 Nonionizing radiation.

a. The RS shall limit the levels of nonionizing radiation of the RS in accordance with SSP 50094.

b. RS transmitters shall not irradiate the Orbiter at levels exceeding the allowable limits as specified in

, Allowable Payload to Orbiter Intentional Electrical Field Strength. A two fault tolerant combination of pointing controls or independent inhibits to transmission may be used to prevent hazardous irradiation of the Orbiter. The inhibits to prevent radiation do not require monitoring unless the predicted radiation levels exceed Orbiter limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.



3.3.6.7 Optics and lasers.

3.3.6.7.1 Lasers.

Lasers used on RS shall be in accordance with SSP 50094.

3.3.6.7.2 Optical requirements.

3.3.6.7.2.1 Optical instruments.

Optical instruments shall prevent harmful light intensities and wavelengths from being viewed by operating personnel.

3.3.6.7.2.2 Personnel protection.

Quartz windows, apertures, or beam stops and enclosures shall be used for hazardous wavelengths and intensities unless suitable protective measures are taken to protect personnel form Ultraviolet or Infrared burns or X-Ray radiation.

3.3.6.7.2.3 Direct viewing optical systems.

Light intensities and spectral wavelengths at the eyepiece of direct viewing optical systems shall be limited to levels below the Maximum Permissible Exposure (MPE).

3.3.6.8 Electrical safety.

3.3.6.8.1 Electrical power circuit overloads.

3.3.6.8.1.1 Circuit overload protection.

Electrical power distribution circuitry shall include protective devices to guard against circuit overloads which could result in distribution circuit damage, excessive hazardous products in pressurized areas and to prevent damage to other safety critical circuits.

3.3.6.8.1.2 Protective device sizing.

Circuit protective devices shall be sized such that steady state currents in excess of the values specified in SSP 50094, paragraph 6.5.1 are precluded.

3.3.6.8.1.3 Bent pin or conductive contamination.

RS electrical design shall ensure that shorts between any pin within a connector that could be caused by a pin bent prior to or during connector mating cannot invalidate more than one inhibit to a hazardous function. Conductive contamination as a similar cause shall be precluded.

3.3.6.8.2 Crew protection for electrical shock.

The crew shall be protected from electrical hazards in accordance with SSP 50094**,** paragraphs 6.5.1.14 to 6.5.1.15.2.5.

3.3.6.8.3 Re application of power.

The RS shall provide local control (See 6.2) of interruption and reapplication of power to each IVA maintenance area.

3.3.6.8.4 Batteries.

RS batteries which can pose a hazard shall be designed in accordance with SSP 50094**,** Section 5.0.

3.3.6.9 Liquid propellant propulsion systems.

3.3.6.9.1 Inadvertent engine firings.

The design and operations of RS propellant systems shall be constrained by the hazardous consequences of inadvertent engine firings. The consequences of engine firings are dependent upon many factors such as the propellant, plume impingement effects (i.e., contamination, heat flux, loads and moments imparted on the ISS or other space vehicles while docked or in approach corridors), operations being conducted in proximity to the thrusters, collision potential, etc. As a minimum the requirements of paragraphs 3.3.6.1.4.1 and 3.3.6.1.5.1 apply to the control of inadvertent engine firings.

3.3.6.9.1.1 Propellant flow control devices.

The propellant delivery system in RS liquid propellant thruster systems shall contain a minimum of two mechanically independent flow control devices in series to prevent engine firing, or expulsion of propellant through the thrust chambers (i.e., at least one isolation valve that separates the propellant tanks from the remainder of the distribution system, and a thruster valve). In bi-propellant systems, the minimum number of devices apply to both the oxidizer and fuel sides.

3.3.6.9.1.1.1 Thruster valves.

The thruster valves in RS liquid propellant thruster systems shall be designed to return to the closed position in the absence of an opening signal.

3.3.6.9.1.1.2 Operations.

A minimum of two mechanical flow control devices between the propellant tank and a thruster shall be in the closed position, whenever firing of the thruster could result in catastrophic consequences. If the design of the propellant system is such that the effects of firing some thrusters are non hazardous and others are hazardous, the non-hazardous thrusters may be fired provided the appropriate mechanical flow control devices are closed and the appropriate number of electrical inhibits are in place for the hazardous thrusters.

3.3.6.9.1.2 Electrical inhibits.

The minimum number of independent electrical inhibits to prevent inadvertent firing of a thruster shall be consistent with the hazardous consequences as defined in paragraphs 3.3.6.1.4.1 and 3.3.6.1.5.1. One of the electrical inhibits must control the opening of the isolation valve whenever inadvertent firing would result in catastrophic consequences.

3.3.6.9.1.3 Monitoring of electrical inhibits to prevent catastrophic thruster firing.

At least two of the three electrical inhibits to prevent a catastrophic thruster firing shall be monitored with one of those monitors being related to the status of the isolation valve.

3.3.6.9.2 Propellant overheating.

The RS propulsion system components (e.g., heaters, valve coils, etc.) that are capable of heating the propellant above the material/fluid compatibility limits of the system shall be two failure tolerant to overheating.

3.3.6.9.3 Propellant leakage.

Mechanical fittings in RS propulsion systems shall contain at least two seals to prevent leakage of propellant into the on-orbit environment.

3.3.6.9.4 Reserved.

3.3.6.9.5 Plume impingement.

The RS shall be able to maintain attitude control of the ISS and prevent hazardous thruster impingement on the Orbiter or the servicing spacecraft.

3.3.6.9.6 Hazardous venting.

RS propulsion system vents (i.e., relief valves, turbo pump assemblies, etc.) shall perform the venting function without causing an additional hazard to the ISS, Orbiter, or a servicing vehicle.

3.3.6.9.7 Monitoring propulsion system status.

The RS shall provide data related to pressure, temperature, and quantity gauging of RS propulsion system tanks, components, and lines to ISS to monitor system health and safety.

3.3.6.9.8 The RS motion control system.

The RS motion control system shall perform attitude control and reboost functions without inducing loads which exceed the design limit loads specified in SSP 42121 ICD**,** paragraph 3.2.1.7.4.1.

3.3.6.10 Fire protection.

3.3.6.10.1 Manual activation.

The RS shall have the capability for crew initiated notification of a fire event within 1 minute after crew detection.

3.3.6.10.2 Isolation.

The RS shall ensure that isolation of a fire event does not cause loss of functionality which may create a catastrophic hazard.

3.3.6.10.3 Suppression.

The RS shall accommodate the application of a fire suppressant at each enclosed location containing a potential fire source.

3.3.6.10.4 Suppressant.

3.3.6.10.4.1 Suppressant material.

Fire suppressant shall be compatible with Space Station life support hardware.

3.3.6.10.4.2 Toxicity level.

The fire suppressant shall not exceed 1 hour SMAC levels in any isolated elements as given in Table V and shall be non-corrosive.

3.3.6.10.5 Contamination.

Fire suppressant by-products shall be compatible with the space station contamination control capability.

3.3.6.10.6 Portable equipment.

3.3.6.10.6.1 Proximity to entrance.

One PBA and one PFE shall be located in elements less than or equal to twenty-four (24) feet in accessible interior length.

3.3.6.10.6.2 Location within element.

Where the element exceeds twenty four (24) feet in accessible interior length, a set of PBAs and PFEs shall be located within twelve (12) feet of each end of the element.

3.3.6.10.6.3 Set co-location.

At least one PBA shall be located within three (3) feet of each PFE.

3.3.6.10.7 Reserved.

3.3.6.10.8 Reserved.

3.3.6.11 Constraints.

3.3.6.11.1 Pressurized volume depressurization and repressurization tolerance.

3.3.6.11.1.1 Pressure differential tolerance

RS equipment located in pressurized volumes shall be capable of withstanding the differential pressure of depressurization, repressurization, and the depressurized condition without resulting in a hazard **(TBR)** .

3.3.6.11.1.2 Operation during pressure changes

Equipment expected to function during depressurization or repressurization shall be designed to operate without producing hazards **(TBR)**.

3.3.6.11.2 Emergency egress.

The RS shall provide for safe emergency IVA egress to the remaining contiguous pressurized volumes and have the capability to isolate from other flight pressurized volumes within 3 minutes, including closing hatches.

3.3.6.11.3 Translation entry/exit paths.

Compartment and pressurized volume entry/exit paths shall not be impeded. (see 6.2)

3.3.6.11.4 Component hazardous energy provision.

Components which retain hazardous energy potential after the component is turned off, shall be designed to prevent a crewmember conducting maintenance from contacting the energy potential or shall be designed with provisions to allow safing of the potential energy, including provisions, to confirm that the safing was successful.

3.3.6.11.5 Hatch opening.

The RS shall provide the capability to control pressure differential and verify that the environment is within the oxygen, nitrogen and carbon dioxide levels as well as within the SMAC levels of selected compounds from Table 1 and provide visual inspection of the interior of the pressurized volume prior to crew ingress **(TBR)**.

3.3.6.11.6 Hatch operations.

Hatches designed to be operated on-orbit interfacing directly to space vacuum shall be self-sealing (inward opening).

3.3.6.11.7 Pins or detachable parts.

Any detachable parts shall be capable of being restrained or tethered.

3.3.6.11.8 Single crewmember entry/exit.

Hatches shall be operable from either side by a single crewmember.

3.3.6.11.9 Reserved.

3.3.6.11.9.1 Reserved.

3.3.6.11.10 Equipment clearance for entrapment hazard.

Clearance shall be provided for equipment removal and replacement to prevent the creation of a crew entrapment hazard.

3.3.6.11.11 Light fixture.

Light fixtures shall be protected by impact proof plastic diffusers which shall contain all potential glass fragments in the case of lamp breakage. The use of special purpose light fixtures will be agreed to separately.

3.3.6.12 Human factors.

3.3.6.12.1 Internal volume touch temperature.

3.3.6.12.1.1 Continuous contact-high temperature.

Surfaces which are subject to continuous contact with crewmember bare skin and whose temperature exceeds 104 degrees Fahrenheit (40 degrees Centigrade) shall be provided with guards or insulation to prevent crewmember contact.

3.3.6.12.1.2 Incidental or momentary contact-high temperature.

For incidental or momentary contact (30 seconds or less), the following apply:

Crewmember warning - surfaces which are subject to incidental or momentary contact with crewmember bare skin and whose temperatures are between 104 degrees F (40 degrees C) and 113 degrees F (45 degrees C) shall have warning labels that will alert crewmembers to the temperature levels.

Crewmember protection - surface temperatures which exceed 113 degrees F (45 degrees C) shall be provided with guards or insulation that prevent crewmember contact.

3.3.6.12.1.3 Internal volume low touch temperature.

When surfaces below 41 degrees F (5 degrees C) which are subject to continuous or incidental contact, are exposed to crewmember bare skin contact, protective equipment shall be provided to the crew and warning labels shall be provided at the surface site.

3.3.6.12.2 External touch temperature for US EVA.

The suit shall be protected from high or low touch temperature extremes as follows:

a. For incidental contact, maintain temperatures within -117 to +113 degrees C (-178.6 to +235.4 degrees F).

b. For unlimited contact within designated EVA crew interface areas as specified in Table XIII and maintain temperatures within -43 to +63 degrees C (-45.4 to +145.4 degrees F).

TABLE XIII. Designated extravehicular activity interfaces
EVA tools and support equipment
EVA translation aids (e.g. CETA cart, handrails, handholds, etc.)
TABLE XIII. Designated extravehicular activity interfaces - Continued
EVA restraints (foot restraints, tethers, tether points etc.)
All EVA translation paths (handrails or structure identified for use as a translation path
All surfaces identified for operating, handling, transfer, or manipulation of hardware
EVA stowage
EVA work site accommodations (handholds, APFR ingress aids, EVA lights, etc.)
EVA ORU handling and transfer equipment

3.3.6.12.3 External edge, corner, and protrusion radii.

a. RS equipment, structures along translation routes, worksite provisions, and each equipment item requiring an EVA interface shall provide rounded corners and edges or edge guards in accordance with Table XIV.

TABLE XIV. Edge, corner, and protrusion criteria - edge and in-plane corner radii(1)

Application			Radius				Remarks
(a)	Openings, panels, covers (corner radii in plane of panel)		0.25 0.12	6.4 3.0	0.12 0.06	3.0 1.5	Preferred Minimum
(b)	Exposed corners:		0.50	13.0			Minimum
(c)	Exposed edges:	(1) 0.08 in. (2.0 mm) thick or greater	0.04 ≥ 1.0				Minimum
		(2) 0.02 to 0.08 in. (0.5 to 2.0 mm) thick	Full Radius		-	-	
		(3) less than 0.02 in. (0.5 mm) thick	Rolled or Curled				
(d)	Small hardware operated by the pressurized-gloved hand		0.04	1.0	-	-	Minimum required to prevent glove snagging
(e)	Small protrusions (less than approximately 3/16 in. (4.8mm)		0.04	1.0	-	-	Absolute minimum unless protruding corner is greater than 120 degrees

NOTE:

(1) A 45 degree chamfer by 0.06 inches (1.5 mm) (minimum) with smooth broken edges is also acceptable in place of a corner radius. The width of chamfer should be selected to approximate the radius corner described above.

b. External RS equipment that will go into a pressurized volume for planned maintenance or storage shall meet the requirements specified in paragraph 3.3.6.12.4.

3.3.6.12.4 IVA internal corner and edge protection.

RS equipment exposed to crew during nominal activity and planned maintenance activity shall be designed to protect the crew from injury by having a minimum of 0.039 inch (1 mm) radius or chamfered edges and corners.

3.3.6.12.5 Reserved.

3.3.6.12.6 Latches.

3.3.6.12.6.1 Design.

Latches or similar devices shall be designed to prevent entrapment of crewmember appendages.

3.3.6.12.6.2 Protective covers or guards.

A protective cover or guard shall be used where suitable substitutes cannot be found.

3.3.6.12.7 Screws and bolts.

Screws or bolts with exposed threads protruding greater than 0.078 inches (2 mm) shall have protective features which include protective covers or rounded edges per 3.3.6.12.4 and that do not prevent installation or removal of the screw or bolt.

3.3.6.12.8 Safety critical fasteners.

Safety critical fasteners shall be designed to prevent their inadvertent back out.

3.3.6.12.9 Levers, cranks, hooks and controls.

Levers, cranks, hooks and controls shall be located such that they cannot pinch, snag, cut, or abrade the crewmembers or their clothing.

3.3.6.12.10 Burrs.

Exposed surfaces shall be smooth and free of burrs.

3.3.6.12.11 Reserved.

3.3.6.12.11.1 Reserved.

3.3.6.12.11.2 Reserved.

3.3.6.12.12 Protrusions.

Equipment except for translation aids identified in Table XIII shall not protrude into the 1 meter (39.4 inches) cylindrical envelope of the secondary translation path.

3.3.6.12.13 Pinch points.

Equipment located outside the habitable volume which pivot, retract, or flex such that a gap of less than 1.4 inches exists between the equipment and adjacent structure shall be designed to prevent entrapment of EVA crewmember appendages.

3.3.6.12.14 Emergency ingress for a non-impaired crew member.

The RS shall provide conditions for emergency ingress into the airlock of a non-impaired crew member within 30 minutes.

3.3.6.12.15 Flex hoses, lines, and cables.

All flex hoses, lines, and cables shall be tethered or otherwise captured to prevent injury to crew and damage to adjacent hardware.

3.3.6.12.16 Translation routes and established worksites.

3.3.6.12.16.1 Primary translation routes and established worksites.

a. Primary translation routes and established worksites shall not pose a risk to EVA crew.

b. External hardware, exposed to the EVA crew along the primary translation route and established worksites, shall not be sensitive to EVA loads.

3.3.6.12.16.2 Secondary translation routes and established worksites.

External hardware along secondary translation routes and established work sites posing a risk to EVA crew shall be placarded (See 6.2) and controlled as specified in Table XV.

TABLE XV. External hardware placards and controls

RISK TYPE	HAZARD	CONTROL METHOD
Innate Characteristics	Non-Ionizing Radiation (Antenna transmit at 15 GHz)	Warning Strips and Placards
	Retract/Rotating Parts	Warning Strips and Placards
	Propulsion/Thrusters	Warning Strips and Placards
	Electrical/Contactors	Warning Strips and Placards
	Thermal (>235F, or <-180F for 0.5 sec)	Warning Strips and Placards
	Stored Energy Devices/Pyrotechnics	Warning Strips and Placards
	Venting of Corrosives	Warning Strips and Placards
By Design	Sharp Edges/Corners	Placards
	Narrow Passageways Protrusions	Placards
	Structures Sensitive to EVA Loads	Placards
	Pinch Points	Placards
	Non-corrosive Contaminants	Placards
	Abrasion Areas	Placards

3.3.6.12.16.3 EVA crewmember contact isolation.

RS hardware with EVA contact hazards which cannot be controlled by design shall be isolated to preclude EVA crewmember contact.

3.3.6.12.17 Moving or rotating equipment.

The EVA crewmember shall be protected from moving or rotating equipment.

3.3.6.12.18 Reserved.

3.3.6.13 Launch vehicle transport - Space Shuttle launch.

The following requirements in section 3.3.6.13 apply only to RS hardware that will be launched on the Space Shuttle:

3.3.6.13.1 Safe without Space Shuttle (SS) program services.

If the RS receives safety critical services from the Orbiter, the RS shall maintain the following capabilities:

3.3.6.13.1.1 Fault tolerance/safety margins.

The RS shall have the capability to maintain fault tolerance or established safety margins consistent with the hazard potential without ground or flight services from the Space Shuttle Program.

3.3.6.13.1.2 Termination of services due to Orbiter emergency conditions.

During Orbiter emergency conditions, RS shall have the capability to achieve and confirm a safe condition within 15 minutes upon notification from the Orbiter to terminate services.

3.3.6.13.2 Critical Orbiter services.

When Orbiter services are to be utilized to control RS hazards, the integrated system shall meet the requirements specified in 3.3.6.1.1 Catastrophic hazards, 3.3.6.1.2 Critical hazards, 3.3.6.1.4, Control of critical hazardous functions and 3.3.6.1.5 Control of catastrophic hazardous functions.

3.3.6.13.3 Inadvertent deployment, separation, and jettison functions.

Inadvertent deployment, separation or jettision of RS hardware or an appendage to that hardware which could result in a collision with the Orbiter or an inability to withstand subsequent loads shall be one or two failure tolerant consistent with the hazard level in accordance with paragraphs 3.3.6.1.1 and 3.3.6.1.2. The general inhibit and monitoring requirements of paragraphs 3.3.6.1.4, 3.3.6.1.5, 3.3.6.2.2, 3.3.6.2.3, and 3.3.6.2.4 apply.

3.3.6.13.4 Planned deployment/extension functions.

3.3.6.13.4.1 Violation of Orbiter payload door envelope.

If a component of the RS or any RS Orbital Support Equipment (OSE) violates the Orbiter payload bay door envelope, the hazard of preventing door closure shall be controlled by independent primary and backup methods.

3.3.6.13.4.2 Method of fault tolerance.

The combination of the primary and backup methods to clear the Orbiter payload door envelope shall be two-fault tolerant. Two methods shall be considered independent if no single event or environment can eliminate both methods (i.e., the methods have no common cause failure mode).

3.3.6.13.5 Contingency return and rapid safing.

The RS shall be designed such that it does not preclude the Orbiter from safing the orbiter payload bay for door closure and deorbit, when emergency conditions develop. These requirements are that: 1) for emergency deorbit, the payload bay doors can be closed within 20 minutes with the deorbit burn in 30 minutes; and 2) for a next primary landing site contingency deorbit, the payload bay doors would be closed no sooner than 50 minutes after declaration of the contingency and deorbit burn would occur 2 hours and 40 minute later. The following requirements shall apply to RS hardware with direct interfaces with the Orbiter.

3.3.6.13.5.1 Emergency deorbit.

The RS hardware shall have at least one system to allow the Orbiter to meet the emergency deorbit requirement. When the Orbiter RMS is utilized for this capability, 10 minutes of the 20 allocated must be allowed for non-RS hardware operations.

3.3.6.13.5.2 Next primary landing site contingency deorbit.

The RS hardware shall have a single failure tolerant capability to allow the Orbiter to meet the next primary landing site contingency deorbit requirement. When RMS utilized for this capability, 10 minutes of the 50 allocated must be allowed for non-RS hardware operations.

3.3.6.13.6 Flammable atmosphere.

3.3.6.13.6.1 Normal functions.

During Orbiter entry, landing, and postlanding operations (whether planned or contingency), the normal (no failures) RS functions shall not cause ignition of a potential flammable payload bay atmosphere.

3.3.6.13.6.2 Electrical ignition sources.

Electrical ignition sources shall not be exposed.

3.3.6.13.6.3 Surface temperatures.

Surface temperatures shall be below 352 degrees F (177.7 degrees C).

3.3.6.13.6.4 Conductive surfaces.

Conductive surfaces (including metalized MLI layers) shall be electrostatically bonded as specified in SSP 50094.

3.3.6.13.7 Allowable RF radiation levels

RS transmitters, located in or out of the Orbiter payload bay, which have the capability to emit radiation levels impinging on the Orbiter exceeding the allowable limits as specified in SSP 50094 shall require three independent inhibits to prevent inadvertent transmission. For transmitters located in the Orbiter payload bay, no radiation is permitted when the payload bay doors are closed and only two inhibits are required when radiation levels are predicted to be below the ICD limits. Inhibits are not required when there is no physical connection to the transmitter power source. The inhibits to prevent inadvertent radiation do not require monitoring unless the predicted radiation levels exceed SSP 50094 limits by more than 6 decibels (dB) in which case two of three inhibits must be monitored.

3.3.6.13.8 Lightning protection.

RS electrical circuits may be subjected to the electromagnetic fields described in SSP 50094, due to a lightning strike to the launch pad. If circuit upset could result in a catastrophic hazard to the STS, the circuit design shall either be hardened against the environment or insensitive devices (relays) added to control the hazard.

3.3.6.13.9 Orbiter vent/dump provisions.

3.3.6.13.9.1 Release or ejection of hazardous materials.

RS hazardous materials shall not be released or ejected which present a hazard to the Orbiter or ISS.

3.3.6.13.9.2 Fluid system containment.

RS hazardous or nonhazardous fluid systems shall contain the fluids unless the use of the Orbiter vent/dump provisions has been negotiated with the Space Shuttle Program Office.

3.3.6.13.10 Sealed compartments.

RS components, located in regions of the Orbiter other than the habitable volume shall be designed to withstand the decompression and recompression environments associated with ascent and descent without resulting in a hazard.

3.3.6.14 Ground interfaces and services - Space Shuttle launch.

Hazards shall not be created due to the inaccessibility of flight hardware such as the following:

3.3.6.14.1 Moving parts.

Moving parts such as fans, belt drives, turbine wheels, and similar components that could cause personnel injury or equipment damage due to inadvertent contact or entrapment of floating objects shall be provided with guards or other protective devices.

3.3.6.14.2 Equipment requiring adjustment.

Equipment requiring adjustment during its operation shall have external adjustment provisions and provide electrical shock protection when applicable.

3.3.6.14.3 Ignition of adjacent materials.

Electrical equipment shall not cause ignition of adjacent materials.

3.3.6.14.4 Accidental contact with electrical equipment.

Electrical equipment shall be designed to provide personnel protection from accidental contact with alternating current (AC) voltages in excess of 30 volts root mean square (rms) or 50 volts direct current (DC) or any lower voltage that could cause injury.

3.3.6.15 Ground interfaces and services - Russian launch vehicle.

RS shall use RS ground processing specifications.

3.3.6.16 Ground support equipment safety requirements for SS launch of RS hardware.

The RS ground support equipment designated to be processed at the Space Shuttle launch site shall be in accordance with SSP 50094.

6.2 Definitions.

CATASTROPHIC HAZARD: Any hazard which may cause a disabling or fatal personnel injury, or cause loss of one of the following: the Orbiter, ISS, or major ground facility. For safety failure tolerance considerations, loss of the ISS is to be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.

CREDIBLE FAILURE: An event that has a potential of occurring based on actual failure modes in similar systems.

CRITICAL HAZARD: Any hazard which may cause a non disabling personnel injury, severe occupational illness; loss of a major ISS element, on-orbit life sustaining function or emergency system; or involves damage to the Orbiter or a ground facility. For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the critical path for station survival or which can be restored through contingency repair.

DESIGN FOR MINIMUM RISK: Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance criteria. The failure tolerance criteria of paragraph 3.3.6.1.1 and 3.3.6.1.2 shall only be applied to these designs as necessary to assure that credible failures that may affect the design do not invalidate the safety related properties of the design. For example, a pressure vessel shall be certified safe based upon its inherent properties to withstand pressure loading that have been verified by analysis and qualification and acceptance testing; however, failure tolerance criteria must be imposed upon external systems that might affect the vessel, such as a tank heater, to assure that failures of the heater do not cause the pressure to exceed the maximum design pressure vessel. Examples are structures, pressure vessels, pressurized lines and fittings, functional pyrotechnic devices, material compatibility, flammability, etc.

FIRE EVENT: Localized or propagating combustion, pyrolysis, smoldering or other thermal degradation processes, characterized by the potentially hazardous release of energy, particulates, or gasses.

FIRE PROTECTION (FP) LOCATION: Any rack , standoff, endcone, cabin, or other area containing powered equipment. FP locations may be closed or open.

HAZARD: The presence of a potential risk situation caused by an unsafe act or condition. A condition or changing set of circumstances that presents a potential for adverse or harmful consequences; or the inherent characteristics of any activity, condition or circumstance which can produce adverse or harmful consequences.

HAZARD CONTROLS: Design or operational features used to reduce the likelihood of occurrence of a hazardous effect. Hazard controls are implemented in the following order of precedence:

a. Elimination of the hazard through removal of hazardous sources and operations.

b. Ensure inherent safety through provisions of appropriate design features, materials and parts selection, and safety factors. Design considerations to include damage control, containment, isolation of potential hazards, and failure considerations.

c. Reduce hazard to an acceptable level by incorporating safety devices as part of the system, subsystem, or equipment.

d. Minimize the effects of potential hazards through the use of warning devices, crew operational procedures, or protective clothing and/or equipment.

HAZARDOUS COMMAND: A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard such as the removal of a required safety inhibit to a hazardous function.

IGNITION SOURCE: An energy release capable of initiating a fire event.

IMPEDE: To obstruct or delay the progress or activation of a function.

IMPEDED: (past tense of impede) - to obstruct or delay the progress of.

INDEPENDENT INHIBIT: Two or more inhibits are independent if no single credible failure, event, or environment can eliminate more than one inhibit.

INDEPENDENT SAFING ACTION: An independent safing action is an action generated by a non failed component which is independent from the failed component being monitored. Any two safing actions are independent if no single fault can prevent both safing actions from transitioning the system to a safe state.

INHIBIT: A design feature that provides a physical interruption between an energy source and a function (such as a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster).

INTERLOCK: A design feature that ensures that any conditions perquisite for a given function or event are met before the function or event can proceed.

LOCAL CONTROL: A capability to accomplish a function at the direction of the crew within the applicable on-orbit module and also prevent reconfiguration of the function by an external entity during the specified period.

NEAR REAL TIME MONITORING: Notification of changes in inhibit or safety status on a periodic basis (nominally once per orbit). The capability of the hardware and software to provide the updated data for near real-time monitoring data is generally the lowest available frequency with normal telemetry, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

OPERATOR ERROR: An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard. The intent is not to include all possible actions by a crew person that could result in an inappropriate action but rather to limit the scope of error to those actions which were inadvertent errors such as an out-of-sequence step in a procedure or a wrong keystroke or an inadvertent switch throw.

PLACARD: A written announcement for display in a public place.

PLACARDED: (past tense of placard) - to post placards on or in. A placard is a printed or written announcement for display in a public place.

RAPID SAFING: The capability of the shuttle to accomplish an emergency de-orbit or a de-orbit contingency to the next primary landing site.

REAL TIME MONITORING: Notification of changes in inhibit or safety status to the crew within a time frame at or near the time the change in status occurred. The frequency requirements of the hardware and software to provide the updated data for real-time monitoring is driven by the ability of the monitoring user to react to the change in status to implement appropriate safing responses, but will be determined on a case-by-case basis depending on the time to effect of the hazard.

RISK: Exposure to the chance of injury or loss. Risk is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity.

SAFE: A general term denoting an acceptable level of risk, relative freedom from and low probability of: personal injury, fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

SAFETY CRITICAL: A characteristic of a condition, event, operation, process, function, equipment or system (including software and firmware) with potential for personnel injury or loss, or with potential for loss or damage to vehicles, equipment or facilities, loss or excessive degradation of the function of critical equipment, or which is necessary to control a hazard.

SAFING: An action or sequence of actions necessary to place systems, subsystems or component parts into predetermined safe conditions.